BRUCE E. MESERVE

Conceptos fundamentales de álgebra



Ediciones de la
UNIVERSIDAD DE CHILE

Conceptos fundamentales de álgebra

CONCEPTOS FUNDAMENTALES DE ALGEBRA

por *Bruce E. Meserve*

Título original: *Fundamental Concepts of Algebra*

Versión castellana publicada por convenio entre la
Universidad de Chile y Addison-Wesley Publishing Company, Inc., EE. UU.

Traducción de *Amalia Villarroel,*
Profesora de Estado.

Obra editada por acuerdo de la
COMISION CENTRAL DE PUBLICACIONES
DE LA UNIVERSIDAD DE CHILE

Edición al cuidado del profesor *Félix Schwartzmann.*

Library of Congress Catalog Nº 52-12052.

Composición: Linotype Baskerville 10/12.
Papel: Hilado especial de la Cía. Manufacturera de Papeles y Cartones.
Impreso en los talleres de la EDITORIAL UNIVERSITARIA, S. A.
San Francisco 454. Santiago, Chile.

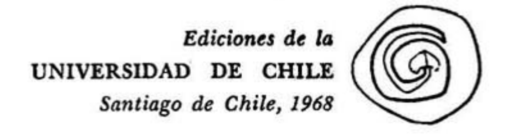
Proyectó la edición *Mauricio Amster.*
Portada de *Hernán Valdés.*
PRINTED IN CHILE

BRUCE E. MESERVE

Conceptos fundamentales de álgebra

Traducción de AMALIA VILLARROEL

Ediciones de la
UNIVERSIDAD DE CHILE
Santiago de Chile, 1968



Indice

Nota preliminar de la traductora 9
Prólogo 12

Capítulo I. NUESTRO SISTEMA DE NÚMEROS

I-1 Conjuntos 13
I-2 Los números cardinales . . 15
I-3 Relaciones de equivalencia . 20
I-4 Los postulados de Peano . . 22
I-5 La adición y la multiplicación 24
I-6 Relaciones de orden . . . 29
I-7 Números inversos y operaciones inversas 31
I-8 Los números racionales positivos 33
I-9 Los números negativos . . 37
I-10 Los números reales . . . 42
I-11 Los postulados de los números reales 46
I-12 Propiedades de los números reales 50
I-13 Los números cardinales transfinitos 56
I-14 Grupo: sistema de números . 60
I-15 Los números complejos . . 63
I-16 Propiedades de los números complejos 69
I-17 Teorema de De Moivre . . 74
I-18 Campos y sistemas de números 79

Capítulo II. TEORÍA DE LOS NÚMEROS

II-1 Divisibilidad 86
II-2 El algoritmo de la división . 88
II-3 Números primos 91
II-4 Teorema de la factorización única 96
II-5 El algoritmo de Euclides . 101
II-6 Bases 106
II-7 Notación decimal 113
II-8 Congruencias 116
II-9 Clases residuales. Función ϕ de Euler 120
II-10 Evaluación de ϕ (m) . . . 124
II-11 Congruencias lineales . . . 127
II-12 Problemas diofánticos . . 131

Capítulo III. TEORÍA DE LOS POLINOMIOS

III-1 Polinomios 135
III-2 Anillos de polinomios . . . 137
III-3 Funciones racionales . . . 139
III-4 Divisibilidad 140
III-5 El algoritmo de la división . 142
III-6 Polinomios irreducibles . . 145
III-7 El algoritmo de Euclides . 148
III-8 Cambio de variable . . . 151
III-9 Ideales 153
III-10 Funciones 154
III-11 Límites 158
III-12 Continuidad 163
III-13 Funciones continuas . . . 166
III-14 Derivadas 170
III-15 Serie de Taylor 173
III-16 Funciones analíticas . . . 175

Capítulo IV. TEORÍA DE LAS ECUACIONES

IV-1 Ceros de un polinomio . . 178
IV-2 División sintética 179
IV-3 Cambio de variable . . . 181
IV-4 Número de raíces 183
IV-5 Determinación de las raíces 185
IV-6 Raíces imaginarias conjugadas 187
IV-7 Polinomios elementales simétricos 188
IV-8 Transformaciones de raíces . 191
IV-9 Ecuaciones cúbicas . . . 196
IV-10 Ecuaciones de cuarto grado . 200
IV-11 La regla de Descartes para los signos 202
IV-12 Teorema de Sturn 207
IV-13 Raíces múltiples 212
IV-14 Soluciones aproximadas . . 217

Capítulo V. DETERMINANTES Y MATRICES

v-1 Desarrollo histórico . . . 221
v-2 Matrices 223
v-3 Permutaciones 225
v-4 Inversiones 227
v-5 Transposiciones 229
v-6 Permutaciones pares e impares 232
v-7 Determinantes 234
v-8 Propiedades de los determinantes 239
v-9 Desarrollo de los determinantes 245
v-10 Determinantes menores . . 252
v-11 Regla de Cramer 260
v-12 Sistemas de ecuaciones lineales 264
v-13 Dependencia lineal 268
v-14 Aplicaciones en geometría analítica 275
v-15 Transformaciones geométricas 279

Capítulo VI. CONSTRUCCIONES

vi-1 Construcciones clásicas . . 289
vi-2 Construcciones clásicas elementales 290
vi-3 El punto de vista algebraico 292
vi-4 Construcciones clásicas básicas 293
vi-5 Construcciones de raíces de ecuaciones 296
vi-6 Problemas de construcción famosos 299
vi-7 Trisecciones geométricas no clásicas 303
vi-8 Trisectores de ángulo mecánicos 306
vi-9 Polígonos articulados . . . 308
vi-10 Resumen 310

Capítulo VII. REPRESENTACIONES GRÁFICAS

vii-1 Los espacios euclidiano y complejo 313
vii-2 Polinomios 315
vii-3 Secciones cónicas 218
vii-4 Superficies cuádricas . . . 323
vii-5 Curvas planas de grado superior 327
vii-6 Funciones racionales . . . 329
vii-7 Funciones algebraicas . . . 334
vii-8 Trazado de curvas 336
vii-9 Gráficos especiales 241
vii-10 Soluciones gráficas 343
vii-11 Determinación de curvas . . 345
vii-12 Conclusión 349

Bibliografía 351
Indice alfabético 355
Símbolos y notas 363

Nota preliminar de la traductora

Para iniciar en el estudio del álgebra a los alumnos universitarios, existen numerosos textos –tanto en castellano como en otros idiomas– que presentan las materias en forma sistemática. Pero el texto escrito por el profesor Bruce E. Meserve difiere notablemente de esas obras, porque elude el tratamiento sistemático del análisis algebraico y presenta aquellos conceptos fundamentales que confieren unidad a la matemática y que por ser tan generales, se encuentran en todas las ramas de esta ciencia.

Pocos textos de matemática tienen el atractivo que posee este libro, cuyo acierto principal es, sin lugar a dudas, la nueva orientación que da a las materias, al presentar el estudio de los temas del álgebra clásica desde el punto de vista del álgebra moderna, en forma tan general, que ésta sirve de enlace entre las dos posiciones.

El lenguaje sencillo y claro –reflejo, sin duda, del empleado por el autor en sus largos años de docencia–, contribuye a prestarle ese atractivo, al mismo tiempo que realza su valor didáctico. La traductora se ha esforzado por conservar estas cualidades en la versión castellana.

AMALIA VILLARROEL BASCOPÉ

Prólogo

El presente libro se basa sobre un curso de álgebra, que forma parte de aquél que bajo el título de "Conceptos fundamentales de matemáticas" se ha estado desarrollando en la Universidad de Illinois en el transcurso de los últimos cuarenta años. En él se presentan y se aplican los temas de análisis junto con los de álgebra. El curso en referencia se completa con otro volumen dedicado principalmente a conceptos fundamentales de geometría.

Se ha adoptado aquí un punto de vista moderno del álgebra y del análisis, es decir, se reconoce la necesidad básica de conocer los conceptos fundamentales de estas materias, fuera de lo que proporcionan los cursos especializados de cada una de sus muchas subdivisiones. Dicha necesidad la experimentan sobre todo los futuros profesores de matemáticas de nivel secundario, los estudiantes de nivel pre-universitario que se preparan para cursos superiores especializados de matemáticas y cualquiera persona que desee una amplia educación liberal.

Durante varios años el autor y otros han empleado como texto la versión mimeografiada de este libro en el nivel superior pre-universitario y en los cursos de graduados*. La mayoría de los estudiantes de este nivel han estudiado, previamente, matemáticas (*college mathematics*) hasta el cálculo. Sin embargo, este libro también se ha empleado con éxito en aquellos casos en que no se exigía el cálculo como requisito previo. Hay abundante material para un curso de cuarenta y cinco horas de clase.

*El texto dice "advanced undergraduate-graduate level". (N. de la T.).

Al tratar el sistema de números complejos y las teorías elementales de números, polinomios y ecuaciones (Cap. I a IV) se aplican los conceptos y la terminología del álgebra moderna. Los Capítulos V (Determinantes y Matrices) y VI (Construcciones) dependen de los primeros cuatro capítulos, pero son independientes entre sí. El vasto alcance de este libro se debe a que se han considerado principalmente los conceptos fundamentales dentro de las diversas materias. Estos conceptos se ilustran con numerosos ejemplos y frecuentemente la teoría se amplía mediante series adecuadas de ejercicios. Este libro se preocupa principalmente de los conceptos fundamentales de las matemáticas superiores (álgebra y análisis) en su relación con las matemáticas elementales. De esta manera, pretende introducir los conceptos de las matemáticas superiores y lograr así que el lector adquiera un conocimiento acabado de las matemáticas elementales.

El autor expresa sus agradecimientos al profesor E. B. Lytle, al profesor Echo Pepper y a la profesora J. H. Chanler, por su contribución al desarrollo del curso que dio origen a este libro. Cabe agregar que la profesora Chanler ha empleado como texto, en sus clases, la versión mimeografiada de este libro e hizo muchas sugerencias valiosas durante toda la preparación del manuscrito.

También debo agradecer las críticas constructivas de muchos alumnos, al profesor F. E. Hohn, que leyó el manuscrito, a mi esposa, que dactilografió el manuscrito, y a los editores por su cooperación y su eficiente desempeño. El autor está sinceramente agradecido de todos y de cada uno de ellos.

BRUCE E. MESERVE

Diciembre, 1952.

CAPITULO I

Nuestro sistema de números

Casi todo el mundo emplea diariamente un sistema de números, sin embargo, pocos pueden describir con exactitud lo que es un sistema de números. En este capítulo nos esforzaremos por conseguir una apreciación correcta de lo que son los números y algunas de sus relaciones entre ellos. A continuación se presenta un método de estudio de los tres sistemas de números que se usan más corrientemente hoy día: los números racionales, los números reales y los números complejos. Durante este estudio resultará evidente que estos tres sistemas se relacionan de modo que los números reales comprenden a los números racionales, y los complejos comprenden a los reales y a los racionales. Se mencionarán, brevemente, algunos otros sistemas de números.

I-1 CONJUNTOS. Los números se asocian frecuentemente a conjuntos de objetos. Tres hombres, tres piedras, tres troncos, tienen una propiedad común que pudo haberse indicado primitivamente por ///. Presentaremos unas cuantas propiedades de los números en términos de conjuntos (se definen oportunamente) y de correspondencias entre conjuntos. Más adelante, adoptaremos algunos postulados como base para un estudio más completo de los números.

El concepto de conjunto, clase, colección de elementos es fundamental, no solamente en matemáticas, sino también en la vida diaria. Por ejemplo, uno a menudo se refiere a un par de zapatos, a un juego de palos de golf, a un juego de piezas de ajedrez, a una

baraja de naipes, a una colección de libros, a un juego de neumáticos para un automóvil, etc. En matemáticas se podría considerar el conjunto de números enteros positivos, los tres vértices de un triángulo, las raíces de una ecuación polinomia, el conjunto de números enteros positivos pares menores que 1.000, el conjunto de números primos positivos, la totalidad de los números reales, etc. En rigor, parafraseando a G. Cantor, definiremos un *conjunto** S como la reunión en un todo de objetos percibidos o considerados distintos; estos objetos se denominan los *elementos* de S. En la práctica, el lector logrará comprender todo el significado e importancia de este concepto (así como de muchos otros), a medida que se haga mayor uso de él.

Los números que el hombre primitivo usó primero para contar los elementos de un conjunto de objetos se llaman *números naturales* o *números enteros positivos.* Técnicamente, los números enteros positivos son símbolos. Pueden escribirse como /, //, ///, ...; i, ii, iii, ...; 1, 2, 3, ...; o de muchas otras maneras. Existen también muchos otros símbolos, tales como 0, -3, $\sqrt{2}$, y π, que más adelante definiremos como números; es decir, ampliaremos el significado de "número" para incluir símbolos que no son enteros positivos. Sin embargo, consideraremos primero algunas de las propiedades básicas de los números enteros positivos.

Cuando los enteros positivos se usan para contar los elementos de un conjunto, suelen llamarse *números ordinales;* cuando se emplean para designar el número de elementos de un conjunto, se llaman *números cardinales.* Consideraremos el concepto de número cardinal en términos de las propiedades comunes de los conjuntos, de cualquier clase de conjuntos que tengan el mismo número cardinal.

La propiedad común a los conjuntos de tres hombres, tres piedras, tres troncos, pudo haberse observado por primera vez cuando cada hombre tenía una piedra en su mano o estaba sentado en un tronco. Esta propiedad común se comprende más fácilmente si se expresa por medio de correspondencias biunívocas, otro concepto fundamental de las matemáticas. Existe una *correspondencia biunívoca* entre los elementos de los conjuntos A y B, siempre que cada elemento del conjunto A corresponda exactamente

*En el presente texto se indicarán con letra cursiva los términos nuevos al ser definidos o identificados por primera vez.

a un elemento del conjunto B y cada elemento del conjunto B sea el correspondiente de exactamente un elemento del conjunto A. El número cardinal b de cualquier conjunto B, designa una propiedad común de todos los conjuntos A_a tales que los elementos de cada conjunto A_a puedan coordinarse en correspondencia biunívoca con los elementos de B.

Podemos asociar, el mismo número 3, con cada uno de los conjuntos de hombres, de piedras y de troncos si y sólo si podemos contar los elementos de cada conjunto empleando los enteros 1, 2, 3, es decir, si existe correspondencia biunívoca entre cada conjunto y el conjunto de los enteros positivos 1, 2, 3. De aquí que el número 3 represente una propiedad común a los conjuntos de tres enteros, tres hombres, tres piedras, tres troncos y a cualquier otro conjunto de elementos que puedan coordinarse en correspondencia biunívoca con cualquiera de estos conjuntos. En otras palabras, todos los conjuntos que pueden coordinarse en correspondencia biunívoca con el conjunto 1, 2, 3, tienen una propiedad común que se designa con el número cardinal 3. En este sentido, el número cardinal 3 sirve para denotar cualquier conjunto de esta clase de conjuntos. Este concepto y el concepto de correspondencia biunívoca entre conjuntos, constituye el fundamento de nuestro estudio sobre las propiedades de los números cardinales.

EJERCICIOS

1. Nombrar o describir dos conjuntos de elementos que tengan el número cardinal 4 e indicar cómo se puede establecer entre ellos una correspondencia biunívoca.
2. Repetir el Ejercicio 1 con otro par de conjuntos que tengan el número cardinal 4.
3. Repetir el Ejercicio 1 con el número cardinal 10.
4. Repetir el Ejercicio 1 con el número cardinal 20.

I-2 LOS NUMEROS CARDINALES.

Si para un conjunto dado S de elementos existe un número entero positivo N tal que los elementos de S puedan coordinarse en correspondencia biunívoca con el conjunto de los enteros positivos 1, 2, ..., N, decimos que S es un *conjunto finito* con el número cardinal (finito) N. Si no existe un número entero positivo N que tenga esta propiedad, y si S tiene, por lo menos, un elemento, de-

cimos que S es un *conjunto infinito.* El número cardinal de cualquier conjunto finito puede obtenerse contando los elementos del conjunto, es decir, corresponde al mayor número ordinal que se necesita para contar los elementos del conjunto. El concepto de número cardinal considerado como un representante cualquiera de una clase de conjuntos permite asociar números cardinales transfinitos con conjuntos infinitos (Cap. 1-13).

Las comparaciones entre números cardinales deben concordar con las comparaciones correspondientes entre los conjuntos de elementos representados por los números cardinales. En efecto, los números cardinales a, b, que representan los conjuntos A, B, son iguales (se escribe $a = b$) y se dice que los conjuntos son *equivalentes* si existe una correspondencia biunívoca entre los elementos de los dos conjuntos. El número cardinal a es *menor que* el número cardinal b (se escribe $a < b$) y b es *mayor que* a (se escribe $b > a$), si después de asociar cada elemento de A con un elemento de B (uno a uno) queda, por lo menos, un elemento de B, al que no le corresponde ningún elemento de A, y no existe entonces una correspondencia biunívoca entre los elementos de B y los elementos de A. La segunda condición es superflua, en el caso de los conjuntos finitos, pero necesaria para los conjuntos infinitos. Por ejemplo, si ambos conjuntos A y B comprenden al conjunto de todos los números enteros positivos n, existe una correspondencia biunívoca (n a n) de cada entero consigo mismo y el conjunto A tiene el mismo número cardinal que el conjunto B. Sin embargo, se puede establecer, también, una correspondencia biunívoca (n a $2n$) entre todos los números enteros de A y los números enteros pares de B. En esta correspondencia entre dos conjuntos infinitos quedan elementos de B (los números enteros impares) que no corresponden a ningún elemento de A. Consideraremos este problema en forma más detallada en nuestro estudio sobre los números cardinales transfinitos (Cap. 1-13). Como ejemplo para el caso de conjuntos finitos, sean A el conjunto de alumnos de una clase, y B el conjunto de sillas de la sala de clases. Si cada alumno tiene una silla y cada silla está ocupada por un alumno, entonces $a = b$. Si cada alumno tiene una silla y, por lo menos, queda una silla sin ocupar, entonces $a < b$. Si todas las sillas están ocupadas y, por lo menos, un alumno no tiene silla, entonces $a > b$.

Un conjunto de elementos B se llama *subconjunto* de un con-

junto A, si cada elemento de B es un elemento de A; y se llama un *subconjunto propio* si es un subconjunto y hay, por lo menos, un elemento de A que no es un elemento de B. Un conjunto que no contiene ningún elemento es un *conjunto vacío o nulo* y se considera como un subconjunto de cualquier conjunto. Usando esta terminología, $a = b$ si A es equivalente a un subconjunto de B, y B es equivalente a un subconjunto de A; $a < b$ si A es equivalente a un subconjunto propio de B y B no es equivalente a ningún subconjunto de A. Dados dos conjuntos finitos A y B cualesquiera con números cardinales a, b, podemos comparar los números cardinales por medio de los subconjuntos 1, 2, ..., a y 1, 2, ..., b del conjunto de los números enteros positivos. Sea C el conjunto 1, 2, ..., c de números enteros positivos que se encuentran en ambos subconjuntos. Si $c = a$ y $c \neq b$, entonces $a < b$. Si $c = a$ y $c = b$, entonces $a = b$. Si $c = b$ y $c \neq a$, entonces $b < a$. De esta manera, hemos demostrado que para dos conjuntos finitos A y B cualesquiera con números cardinales a, b, debe ser válida exactamente una de las relaciones siguientes: $a < b$, $a = b$, o bien, $a > b$.

El ejemplo anterior de los alumnos, puede ampliarse para ilustrar la suma de los números cardinales. Sea G^* el conjunto de niñas de la clase, B^* el conjunto de niños, C^* el conjunto de sillas y g, b, c los números cardinales respectivos de estos conjuntos. Si cada estudiante tiene una silla y cada silla está ocupada por un estudiante, entonces, $c = g + b$. En general, dados los conjuntos A, B, C, en que A y B no tienen elementos en común (es decir, que los conjuntos A y B son *mutuamente exclusivos*), podemos escribir $a + b = c$, cuando existe una correspondencia biunívoca entre los elementos de C y la totalidad de los elementos de A y B; en otras palabras, C es equivalente a $A + B$ en que la suma de conjuntos ha de entenderse en el sentido de la teoría de conjuntos, como *totalidad de los elementos*. De esta manera, puede comprenderse fácilmente la adición de dos números cardinales cualesquiera por medio de correspondencias biunívocas. También se puede definir la multiplicación de los números cardinales. La sustracción y la división se pueden definir sólo en casos especiales. Por ejemplo, se puede escribir $c - b = a$, si y sólo si existe un número cardinal a tal que $c = a + b$.

*En inglés G de *girl*, niña; B de *boy*, niño; y C de *chair*, silla. (N. de la T.).

El producto de dos números cardinales, así como el producto de dos números enteros positivos, puede expresarse utilizando el concepto de adición sucesiva: $1 \cdot a = a$, $2 \cdot a = a + a$, $3 \cdot a = a + a + a$, ... Si el número de niños es igual al número de niñas en la clase a que nos referíamos anteriormente, entonces $g = b$ y $c = b + b = 2 \cdot b$. En este caso, el producto $ab = 2b$ es el número cardinal de un conjunto C equivalente a la suma de la totalidad de los elementos del conjunto C_1 de sillas ocupadas por las niñas y del conjunto C_2 de sillas ocupadas por los niños. En general, se escribe $c = ab$, siempre que C sea equivalente a la suma de la totalidad de los elementos de los conjuntos $C_1, C_2, ..., C_a$ mutuamente exclusivos; cada C_i es equivalente a B, y existe una correspondencia biunívoca (que se ha señalado con subíndices) entre los elementos de A y el conjunto de conjuntos C_i. En el ejemplo anterior, C es equivalente a $B + G$, B es equivalente a G, y existe una correspondencia biunívoca entre los elementos de A, por ejemplo, a_1, a_2, y el conjunto compuesto de los elementos B, G. Se puede escribir también $c/b = a$, siempre que $c = ab$.

Las *cuatro operaciones racionales* (adición, sustracción, multiplicación y división) se examinarán ampliamente en el presente texto. En el caso de los números cardinales, se ha visto que la suma de dos números cardinales cualesquiera es un número cardinal; la diferencia entre dos números cardinales es un número cardinal, para los casos en que esté definida; el producto de dos números cardinales cualesquiera es un número cardinal; y el cuociente de dos números cardinales es un número cardinal, siempre que esté definido previamente. Además, nuestras definiciones bastan para permitirnos probar que: a) los números cardinales satisfacen las relaciones corrientes de orden para los números enteros positivos (Ejercicios 7 y 8); y b) que la suma (Ejercicio 9) y la multiplicación (Ejercicio 10) de números cardinales tienen las mismas propiedades básicas que se atribuyen a la suma y multiplicación de los números enteros positivos (Cap. 1-5).

Antes de considerar las propiedades de los números enteros positivos convendría examinar, brevemente, los términos "operación" y "relación". Dado cualquier par de elementos a, b de un conjunto S, a menudo se asocia con ellos otros elementos, tales como $a + b$, $a - b$, $a \cdot b$, a/b de S. Tales operaciones se llaman *operaciones binarias* en S. En general, un conjunto S *es cerrado* bajo

una operación binaria $\oplus$, y la operación está *unívocamente determinada* sobre el conjunto S, si para todos los elementos a, b de S, el elemento $a \oplus b$ es un elemento único de S. Las operaciones binarias de suma y multiplicación ya se han definido sobre el conjunto de números cardinales.

También se pueden comparar dos elementos a y b de un conjunto S. Por ejemplo, $a > b$ y $a = b$ indican comparaciones o *relaciones binarias* entre los elementos de S. Una relación binaria $\ominus$ está definida sobre un conjunto S, si para todo par ordenado (a, b) de elementos de S, puede determinarse si la relación es válida o no. Se dará por aceptado que cualquiera relación binaria debe ser válida o no serlo. Básicamente, supondremos que dados dos números cualesquiera a, b precisamente debe ser válida una de las relaciones $a = b$, o $a \neq b$. En este texto nos ocuparemos de las operaciones binarias y las relaciones binarias. En general, el conjunto S estará determinado: el conjunto S podría ser un conjunto particular de números o un conjunto de polinomios de ciertas variables definidas con coeficientes pertenecientes a un conjunto particular de números. Nos preocuparemos de definir o de indicar las características de todas las relaciones empleadas, teniendo en cuenta sus propiedades fundamentales, es decir, se establecerán propiedades de la relación tales, que todas las proposiciones en que aparezca la relación, serán válidas para todas las relaciones que tengan estas propiedades.

Las operaciones binarias de adición y multiplicación se tratarán de la manera ya descrita, es decir, se intentará caracterizar estas operaciones mediante sus propiedades básicas. En efecto, el desarrollo del sistema de números considerado en este capítulo, es esencialmente una consideración de las propiedades básicas de las relaciones de equivalencia, de los números enteros positivos, de la adición, de la multiplicación, de las relaciones de orden, de los números inversos, de las operaciones inversas, de los números racionales positivos, de los números negativos, de los números reales y de los números complejos. El orden de las materias en este estudio sigue fielmente aquél de la evolución histórica de nuestro sistema de números. La forma de postulados en que se presenta la materia obedece a una formalización matemática relativamente moderna que acentúa los conceptos fundamentales sobre los que se basa el álgebra (véase Bibliografía Nº 10, págs. 221-232). El

modo de abordar la teoría de los conjuntos es también comparativamente reciente (véase Bibliografía Nº 28). En el Nº 17 de la Bibliografía, se encontrará una relación no técnica del desarrollo del concepto de número con muchas anécdotas históricas.

EJERCICIOS

1. Dar un ejemplo de suma de números cardinales utilizando conjuntos de elementos.

2. Dar un ejemplo de sustracción de números cardinales, utilizando conjuntos de elementos.

3. ¿Está determinado $a - b$ para todos los números cardinales? Explicar.

4. Proponer un ejemplo de conjuntos A, B, que satisfagan las siguientes condiciones: (a) $a = b$; (b) $a = 2b$; (c) $a = 4b$; (d) $a < b$.

5. Citar un ejemplo de conjuntos A, B, que satisfagan las siguientes condiciones: (a) que $a - b$ esté definido; (b) que $a - b$ no esté definido; (c) que a/b esté definido; (d) que a/b no esté definido.

6. Valiéndose de sus conocimientos sobre números enteros, indique una correspondencia biunívoca entre los números enteros positivos y (a) los números enteros positivos pares; (b) los números enteros negativos; (c) los números enteros positivos múltiplos de diez; (d) las potencias enteras positivas de dos.

7. Demostrar que para números cardinales a, b, c, cualesquiera se verifica (a) si $a < b$ y $b < c$, entonces $a < c$; (b) si $a < b$, entonces $a + c < b + c$; (c) si $a < b$, entonces $ac < bc$.

8. Definir $a \geqq b$ para números cardinales a, b, cualesquiera y repetir el Ejercicio 7 para la relación $\geqq$

9. Demostrar que para números cardinales a, b, c, cualesquiera: (a) $a + b$ es un número cardinal único; (b) $a + b = b + a$; (c) $(a + b) + c = a + (b + c)$.

10. Demostrar que para números cardinales a, b, c cualesquiera: (a) ab es un número cardinal único: (b) $ab = ba$; (c) $(ab)c = a(bc)$; (d) $(a + b)c = ac + bc$.

1-3 RELACIONES DE EQUIVALENCIA.

Toda relación que tenga las tres propiedades siguientes, es decir, que sea:

reflexiva, $a = a$,
simétrica, $a = b$ implica $b = a$,
transitiva, $a = b$ y $b = c$ implican $a = c$,

se llama una *relación de equivalencia.* Puede demostrarse, como se indica a continuación, que la equivalencia de conjuntos es una relación de equivalencia y, por lo tanto, que la igualdad de números cardinales, tal como se define en el Cap. 1-2, también lo es: es reflexiva, puesto que los elementos de cualquier conjunto pueden ordenarse en correspondencia biunívoca con ellos mismos; es simétrica, dado que cualquiera correspondencia biunívoca entre los elementos de un conjunto A y los elementos de un conjunto B, puede también considerarse como una correspondencia biunívoca entre los elementos del conjunto B y los del conjunto A. Por último, es transitiva, ya que una correspondencia biunívoca entre los elementos de un conjunto A y aquellos de un conjunto B y

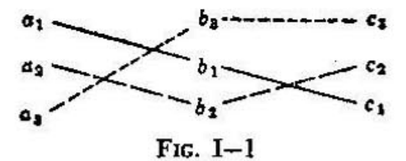


Fig. I–1

una segunda correspondencia biunívoca entre los elementos de B y aquellos de un conjunto C, dan origen a una correspondencia biunívoca entre los elementos de A y aquellos de C. Por ejemplo, en el caso de conjuntos finitos, si designamos los elementos correspondientes de A, B, C por a_i, b_i, c_i, respectivamente, obtenemos correspondencias similares a aquellas que se indican en la Fig. 1-1.

También se puede demostrar, empleando las definiciones acostumbradas, que la "identidad" ($\equiv$), la "congruencia" ($\cong$) de figura geométricas, y la "semejanza" ($\sim$) de figuras geométricas son relaciones de equivalencia. De esta manera, cada uno de los símbolos $=$, $\equiv$, $\cong$, $\sim$ representa "igual a" en un sentido matemático bien definido. Ahora nos serviremos de la relación de equivalencia $=$ para describir las características de los números enteros positivos mediante los postulados de Peano. Como se señaló en el Cap. 1-2, se da por aceptado que dados dos números a y b, debe verificarse exactamente una de las dos relaciones $a = b$, $a \neq b$.

EJERCICIOS

1. ¿Expresa el signo $<$ una relación de equivalencia? Explicar

2. Demostrar que la semejanza de figuras en geometría plana es una relación de equivalencia.

3. ¿Representa el signo $\neq$ una relación de equivalencia? Explicar.

4. Determinar cuáles de las siguientes relaciones entre estudiantes son relaciones de equivalencia: (a) tener la misma edad, por ejemplo: Ruth tiene la misma edad que Juan; (b) ser mayor; (c) tener por lo menos la misma edad que . . .; (d) tener el mismo peso; (e) tener pesos diferentes; (f) tener mejores calificaciones; (g) tener en común una característica cualquiera dada; (h) no tener en común una característica dada.

5. La propiedad de las personas de ser diferentes, ¿es una relación de equivalencia? Explicar.

6. Dar un ejemplo de una relación que sea transitiva, pero que no sea reflexiva ni simétrica.

7. Dar un ejemplo de una relación que sea reflexiva y transitiva, pero no simétrica.

8. Dar un ejemplo de una relación que sea simétrica pero no sea reflexiva ni transitiva.

9. Demostrar que, considerado como conjunto de elementos, el conjunto de los números enteros positivos es equivalente al conjunto de las potencias enteras positivas de diez.

10. Ilustrar la equivalencia entre el conjunto de puntos de un segmento de recta de una unidad de longitud y el conjunto de puntos de un segmento de recta de diez unidades de longitud.

11. Ilustrar la equivalencia entre el conjunto de puntos de una recta y el conjunto de puntos de una circunferencia a la cual se le ha suprimido un punto.

12. Ilustrar la equivalencia entre el conjunto de puntos de un plano y el conjunto de puntos de una esfera a la cual se le ha suprimido un punto.

I-4 LOS POSTULADOS DE PEANO.

Ahora, vamos a iniciar el estudio de nuestro sistema de números siguiendo un orden lógico. En esta sección se formularán, primero, cinco propiedades que pueden usarse para distinguir a los números enteros positivos; en seguida, se dará por aceptado que los números enteros positivos tienen estas propiedades (es decir, estas propiedades se considerarán como postulados para el desarrollo de nuestro sistema de números) y finalmente se empleará uno de estos postulados para obtener un procedimiento formal para demostrar que una relación es válida para todos los números enteros positivos. Las cinco proposiciones siguientes se conocen con el nombre de *postulados de Peano:*

(i) 1 es un entero positivo.

(ii) A cada entero positivo a le corresponde como sucesor un entero positivo único a^+.

(iii) A ningún entero positivo le corresponde 1 como sucesor.

(iv) Si $a^+ = b^+$, entonces $a = b$.

(v) Todo conjunto de enteros positivos que contenga a 1 y al sucesor de todo entero positivo del conjunto, contiene a todos los enteros positivos.

El postulado (v) suele llamarse el *principio de inducción completa* y constituye la base del principio de inducción matemática. Ya que todo entero positivo a tiene un sucesor a^+, no existe un entero positivo mayor que todos los demás y no es posible verificar, por separado, ninguna relación para cada uno y para todos los enteros positivos. Por consiguiente, para demostrar que una relación o proposición es válida para todos los enteros positivos n necesitamos aplicar el principio de inducción completa. Más específicamente, consideramos el conjunto S de enteros positivos para el cual la proposición se verifica (es válida). Si 1 pertenece al conjunto S y, para cada entero positivo k de S, el entero $k^+ = k + 1$ pertenece también a S, entonces, según el principio de inducción completa, todos los números enteros positivos pertenecen al conjunto S, es decir, la proposición es válida para todos los números enteros positivos. He aquí el *principio de inducción matemática:*

Si una proposición $P(n)$ está definida para todos los valores enteros positivos de n de tal manera que $P(1)$ sea válido y que la validez de $P(k)$ implique la validez de $P(k + 1)$ para un valor entero positivo de k elegido arbitrariamente, entonces $P(n)$ es válida para todos los valores enteros positivos de n.

Aquí vamos a hacer una digresión y consideraremos un ejemplo de este principio, aun cuando técnicamente algunas de las operaciones y símbolos, tal como n^2, aún no han sido definidos. Supongamos que la proposición $P(n)$ sea

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

Para $n = 1$ se tiene $P(1): 1 = 1$, lo que es válido. En seguida, sea k cualquier número entero positivo tal que $P(k)$ sea válida, es decir,

$$1 + 3 + 5 + \ldots (2k - 1) = k^2;$$

sumando $2k + 1$ a ambos miembros de esta ecuación, queda demostrada la validez de $P(k + 1)$:

$$1 + 3 + \ldots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2.$$

Luego, según el principio de inducción matemática, la proposición anterior $P(n)$ es válida para todos los valores enteros positivos de n. Otros ejemplos de la aplicación de este principio pueden encontrarse en el conjunto siguiente de ejercicios.

EJERCICIOS

Demostrar las proposiciones de los Ejercicios 1 a 3 aplicando los postulados de Peano. Demostrar las relaciones de los Ejercicios 4 a 9, aplicando el principio de inducción matemática.

1. Si $a \neq b$, entonces $a^+ \neq b^+$.
2. $a^+ \neq a$.
3. Todo entero positivo $a \neq 1$ es de la forma b^+, en que b es un entero positivo.
4. $2 + 4 + 6 + \cdots + 2n = n(n + 1)$.
5. $3 + 6 + 9 + \cdots + 3n = \dfrac{3n(n + 1)}{2}$.
6. $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}$
7. $x - y$ es factor de $x^n - y^n$, siendo n un entero positivo cualquiera.
8. $x^{2n} - y^{2n}$ es divisible por $x + y$, siendo n un número entero positivo cualquiera.
9. $x^{mn} - y^{mn}$ es divisible por $x^m - y^m$ en que m y n son números enteros positivos cualesquiera.

I-5 LA ADICION Y LA MULTIPLICACION. Los postulados de Peano no bastan para definir la adición y la multiplicación explícitamente, pero pueden emplearse para demostrar que cada una de estas operaciones puede definirse exactamente de una manera única que satisfaga ciertas condiciones. Por ejemplo, puede demostrarse (Véase Bibliografía Nº 31; págs. 4-5) que dados dos números enteros positivos cualesquiera a, b, se

puede definir unívocamente un número entero positivo $a + b$, de modo que

$$a^+ = a + 1$$

para todo entero positivo a, y

$$a + b^+ = (a + b)^+$$

para todo par de enteros positivos a, b. Estas dos propiedades de la adición y los postulados de Peano pueden, por esta razón, aplicarse para demostrar que la adición de los números enteros positivos es única, asociativa y conmutativa, es decir,

(i) si a y b son números enteros positivos, existe un entero positivo único c tal que $a + b = c$;

(ii) $(a + b) + c = a + (b + c)$; y
(iii) $a + b = b + a$.

Se indicarán los procedimientos empleados para demostrar estas propiedades. Un examen acabado de esta materia puede encontrarse en el Nº 31 de la Bibliografía; págs. 3-8.

Se demostrará primero que $a + b$ es único para todos los enteros positivos a, b. Sea a un número entero positivo elegido arbitrariamente, pero fijo, y S el conjunto de enteros positivos b tales que $a + b$ sea un entero positivo determinado unívocamente. Por definición y de acuerdo con el segundo postulado de Peano, 1 pertenece a S, ya que $a^+ = a + 1$ es un número entero positivo unívocamente determinado. Si b pertenece a S, entonces $(a + b)^+$ se encuentra unívocamente determinado (segundo postulado de Peano), y b^+ pertenece a S dado que $a + b^+ = (a + b)^+$, de acuerdo con la segunda propiedad de la definición de adición. Por lo tanto, S contiene a todos los números enteros positivos, y $a + b$ es un entero positivo unívocamente determinado para todos los números enteros positivos a, b.

La demostración de que la adición es asociativa se obtiene de un modo similar (Ejercicio 1, más adelante) probando que el conjunto R de enteros positivos c tales que $(a + b) + c = a + (b + c)$ contiene a todos los enteros positivos.

Para demostrar que la adición es conmutativa se requiere dos veces el empleo del principio de inducción completa. Se demuestra primero que $a + 1 = 1 + a$ para todo entero positivo a y luego que $a + b = b + a$ para todos los números enteros positivos a, b. Sea T el conjunto de números enteros positivos a tales que $a + 1 = 1 + a$. El entero 1 pertenece a T dado que $1 + 1 = 1 + 1$. Si a pertenece a T, luego $a + 1 = 1 + a$ y dado que ya se ha demostrado la asociatividad de la adición, se puede aplicar la segunda propiedad de la definición de la adición dos veces y obtener $a^+ + 1 = (a + 1) + 1 = a + (1 + 1) = a + 1^+ = (a + 1)^+ = (1 + a)^+ = 1 + a^+$. Por lo tanto T contiene a^+ y de acuerdo con el principio de inducción completa, el conjunto T contiene a todos los números enteros positivos. Por último, sea a un número entero positivo constante elegido arbitrariamente y sea U el conjunto de los enteros positivos b tales que $a + b = b + a$. Acabamos de demostrar que 1 pertenece a U. Para cualquier número entero positivo b de U, tenemos que $a + b^+ = a + (b + 1) = (a + b) + 1 = 1 + (a + b) = 1 + (b + a) = (1 + b) + a = (b + 1) + a = b^+ + a$, de donde U contiene a todos los números enteros positivos (Ejercicio 2) y se ha demostrado que la adición es conmutativa.

Nos hemos servido de los postulados de Peano y de las dos propiedades de la adición que figuran en la definición de la adición para demostrar que la adición de dos enteros positivos es única, asociativa y conmutativa. Estas cinco propiedades de la adición se usarán extensamente en el desarrollo de nuestro sistema de números. Por ejemplo, se puede demostrar ahora la ley cancelativa de la adición, es decir, que $a + b = a + c$ implica $b = c$ (Ejercicio 3).

El tratamiento de la multiplicación que aquí se indica es muy similar al de la adición. Puede demostrarse (véase Bibliografía Nº 31; págs. 14-15) que, dados dos números enteros positivos a, b cualesquiera, se puede definir unívocamente un número entero positivo que se escribe $a \cdot b$ y también frecuentemente ab, de tal manera que

$$a \cdot 1 = a$$

para todo entero positivo a, y

$$a \cdot b^+ = ab + a$$

para todo par de enteros positivos a, b. Estas dos propiedades de la multiplicación y los postulados de Peano pueden emplearse ahora para demostrar que la multiplicación de los números enteros positivos es única (Ejercicio 6), distributiva con respecto a la adición (Ejercicios 8 y 11), asociativa (Ejercicio 9), y conmutativa (Ejercicios 7 y 10). También se puede demostrar la ley cancelativa de la multiplicación, es decir, que $ab = ac$ implica $b = c$ para números enteros positivos arbitrarios a, b, c (Ejercicio 12). Se dice que un entero d tiene un *factor o divisor* b si y sólo si existe un número entero a tal que $d = ab$. La ley cancelativa de la multiplicación establece por consiguiente que si $d = ab$ y $d = ac$, luego $b = c$.

La *notación exponencial* a^b en que a, b son números enteros positivos cualesquiera, se define como el producto $aaa \ldots a$ de b factores a. Según esta definición $a^b \cdot a^c = a^{b+c}$; si $a = d$, resulta $a^b = d^b$ (Ejercicio 16), y $a^b = d^b$ implica $a = d$ (Ejercicio 17), en que a, b, d son números enteros positivos elegidos arbitrariamente.

La definición $a \cdot 1 = a$ y la ley cancelativa de la multiplicación implican que si $ab = a$, entonces $b = 1$. La propiedad $a \cdot 1 = 1 \cdot a = a$ del número entero positivo 1 (Ejercicio 7) se indica estableciendo que 1 es la unidad, o sea, la *identidad con respecto a la multiplicación*. En general, la *identidad con respecto a una operación* es un elemento que, cuando se aplica a cualquier número de un conjunto dado mediante la operación dada, deja al número invariable. Nos referiremos en forma particular a los elementos de identidad de la adición y de la multiplicación.

Si existiera un número entero positivo b tal que $a + b = a$, entonces tendríamos que $(a + b)^+ = a^+$; $a + b^+ = a + 1$; y $b^+ = 1$, contrariamente al tercer postulado de Peano. Por lo tanto, no existe la identidad con respecto a la adición en el conjunto de los números enteros positivos. En consecuencia, ampliaremos ahora el concepto de "número" e incluiremos un símbolo que no es un entero positivo y definiremos este nuevo símbolo *0*, llamado cero, de tal manera que $a + 0 = a$ y $a \cdot 0 = 0$, donde a es cualquier número entero positivo o cero. Denominaremos a cero un número entero, pero teniendo presente que no es un entero positivo. En consecuencia (Ejercicio 18), con excepción de la ley cancelativa de la multiplicación, las propiedades básicas de la adición y de la multiplicación se verifican para el conjunto de números que comprende a los nú-

meros enteros positivos y cero, es decir, el conjunto de los *enteros no negativos.*

La propiedad $a \cdot 0 = 0$ para cualquier número entero no negativo a y el principio de inducción matemática pueden servir para demostrar que $0^b = 0$ para cualquier entero positivo b (Ejercicio 15). El símbolo 0^0 es *indefinido,* es decir, no tiene un significado específico en nuestro sistema de números. Para cualquier número entero positivo a, se define $a^0 = 1$, con el objeto de conservar la propiedad $a^b a^c = a^{b+c}$ para todos los enteros no negativos b, c. Hasta aquí se ha examinado la igualdad, la adición y la multiplicación de los números enteros positivos. Si a y b son números enteros positivos, resulta que $a = c$, $a + b = d$, y $a \cdot b = e$ son también números enteros positivos, es decir, el conjunto de números enteros positivos es cerrado (Cap. 1-2) con respecto a estas operaciones. En otras palabras, las ecuaciones $a = x$, $a + b = y$, y $a \cdot b = z$ tienen todas soluciones dentro del conjunto de los números enteros positivos. Ya se ha visto que la solución de $a + x = a$ no es un entero positivo. Antes de definir nuevos números con el objeto de encontrar las soluciones de $ax = b$, y $a + x = b$, se considerará un caso especial del segundo problema. En particular, se considerará una ordenación $a < b$ de los números enteros positivos tal que $a < b$ y $b > a$ todas las veces que $a + x = b$ tenga una solución dentro del conjunto de los números enteros positivos.

EJERCICIOS

1. Demostrar que la adición de los números enteros positivos es asociativa.
2. En el ejercicio anterior, al demostrar que la suma es conmutativa, explicar la razón, en cada paso de la demostración, por qué U contiene a todos los números enteros positivos.
3. Demostrar que $a + b = a + c$ implica $b = c$ para números enteros positivos cualesquiera a, b, c.
4. Demostrar que si $a = b$, entonces $a^+ = b^+$ y $a + c = b + c$, en donde c es cualquier número entero positivo.
5. Demostrar que $a = b$ y $c = d$ implican que $a + c = b + d$.
6. Demostrar que ab es un número entero positivo único para números enteros positivos a, b cualesquiera.
7. Demostrar que $a \cdot 1 = 1 \cdot a = a$ para todo número entero positivo a.
8. Demostrar que la multiplicación permanece distributiva con respecto a la adición, es decir, $a(b + c) = ab + ac$.
9. Demostrar que la multiplicación es asociativa, es decir, $(ab)c = a(bc)$.

10. Demostrar que la multiplicación es conmutativa, es decir, $ab = ba$.

11. Demostrar que la multiplicación es distributiva con respecto a la adición, es decir, $a(b + c) = ab + ac = (b + c)a$.

12. Demostrar que $ab = ac$ implica $b = c$ para números enteros positivos cualesquiera a, b, c.

13. Demostrar que $a = b$, implica $ac = bc$, donde c es un número entero positivo cualquiera.

14. Demostrar que $a = b$ y $c = d$ implica $ac = bd$.

15. Demostrar que $0^b = 0$ se verifica para cualquier número entero positivo b.

16. Demostrar que $a = d$ implica $a^b = d^b$, en donde a, d son números enteros no negativos arbitrarios y b es cualquier entero positivo.

17. Demostrar que $a^b = d^b$ implica $a = d$, en que a y d son números enteros no negativos cualesquiera, y b es cualquier número entero positivo.

18. Demostrar que en el conjunto de números enteros no negativos, la suma es única, asociativa y conmutativa, y que la multiplicación es única, asociativa, conmutativa y satisface la ley de distributividad.

I - 6 RELACIONES DE ORDEN.

Los números cardinales se han ordenado principalmente conforme a la definición siguiente: $a < b$ si y sólo si existe un número cardinal c tal que $a + c = b$ (Cap. I - 2). Definiremos ahora una ordenación similar para el conjunto de los números enteros positivos y cero, es decir, para el conjunto de los números enteros no negativos. Dados dos números enteros no negativos cualesquiera a, b se dice que *a es menor que b* ($a < b$) y que *b es mayor que a* ($b > a$) si y sólo si existe un entero positivo c tal que $a + c = b$. De manera que $0 < b$ para todo número entero positivo b (Ejercicio 1), y $1 < b$ para todo número entero positivo $b \neq 1$ (Ejercicio 2).

Dados dos números enteros no negativos cualesquiera a, b, podemos considerar ahora tres relaciones binarias $a < b$, $a = b$, $a > b$. Sea T el conjunto de números enteros no negativos a tales que se verifique exactamente una de las relaciones $a < b$, $a = b$, $a > b$, para todos los números enteros no negativos b. De acuerdo con lo señalado en el Cap. I - 3 se dará por sentado que dados dos enteros a, b, cualesquiera se verifica exactamente una de las relaciones $a = b$, $a \neq b$. Para $a = 0$, se obtiene $0 = b$ si $b = 0$ y $0 < b$ para $b \neq 0$. Para $a = 1$ se obtiene $b < 1$ si $b = 0$, $1 < b$ si $b \neq 0$ y $b \neq 1$. Para cualquier entero a de T se obtiene $b < a^+$ si $b < a$ o $b = a$; $b = a^+$ si $a < b$ y $a + 1 = b$; $a^+ < b$ si $a < b$ y $a^+ \neq b$.

Por consiguiente, de acuerdo con el principio de inducción matemática, todos los números enteros no negativos pertenecen al conjunto T. En otras palabras, dados dos números enteros no negativos cualesquiera a, b, es válida exactamente sólo una de las relaciones $a < b, a = b, a > b$.

La definición ya enunciada de $a < b$ para los números enteros no negativos se usará al definir $a < b$ para los números racionales positivos (Cap. 1-8), para los números negativos (Cap. 1-9) y para los números reales (Cap. 1-11). La ordenación de los números reales puede imaginarse fácilmente si se considera una correspondencia biunívoca entre el conjunto de los números reales y el conjunto de puntos de una recta según la geometría corriente de Euclides. El Axioma de Cantor-Dedekind (Cap. 1-12) establece esta correspondencia biunívoca. En este axioma se basa también el concepto de conjunto ordenado linealmente.

Un conjunto de elementos está *ordenado linealmente* si para elementos a, b del conjunto elegidos arbitrariamente

(i) $a \neq b$ implica $a < b$ o $b < a$;
(ii) $a < b$ implica $a \neq b$; y
(iii) $a < b$ y $b < c$ implican $a < c$.

Se ha dejado como un ejercicio para el lector el demostrar que el conjunto de números enteros no negativos está ordenado linealmente (Ejercicio 3). También puede demostrarse (Ejercicio 4) que exactamente una de las relaciones $a < b, a = b, a > b$ debe verificarse si a y b son elementos de cualquier conjunto ordenado linealmente.

La relación $<$ tiene varias propiedades más si a, b, c, d son números enteros no negativos cualesquiera. Por ejemplo,

(iv) $a < b$ implica $a + c < b + c$;
(v) $a < b$ y $c < d$ implican $a + c < b + d$;
(vi) $0 < c$ y $a < b$ implican $ac < bc$;
(vii) $a < b$ y $c < d$ implican $ac < bd$;
(viii) $1 < a$ y $b \neq 0$ implican $1 < a^b$;
(ix) $d \neq 0$ y $a < b$ implican $a^d < b^d$;
(x) $a < b$ y $1 < d$ implican $d^a < d^b$; y
(xi) $a < b$ y $1 < c < d$ implican $c^a < d^b$.

Las demostraciones de estas propiedades de los números enteros no negativos se dan como ejercicio (Ejercicio 5). Se considerará la validez y las modificaciones necesarias de estas propiedades a medida que nuestro concepto de número se amplíe y que las relaciones binarias $=$ y $<$ se definan para los números racionales positivos, para los números negativos y para los números reales.

EJERCICIOS

1. Demostrar que $0 < b$ para todo entero positivo b.
2. Demostrar que $1 < b$ para todo entero positivo $b \neq 1$.
3. Demostrar que el conjunto de números enteros no negativos está ordenado linealmente.
4. Demostrar que una de las relaciones $a < b$, $a = b$, $a > b$ debe ser válida exactamente si a, b son elementos de un conjunto ordenado linealmente.
5. Demostrar las propiedades (iv) a (xi) de la relación $<$ para los números enteros no negativos.
6. Se dice que un conjunto de elementos está *bien ordenado* si todo subconjunto *no vacío* (es decir, todo subconjunto que contiene por lo menos un elemento) tiene un primer elemento. Demostrar que el conjunto de números enteros no negativos es bien ordenado, es decir, demostrar que si un subconjunto de los números enteros no negativos contiene por lo menos un elemento, entonces contiene un elemento b tal que $b \leqq n$ para todo elemento n del subconjunto.

I-7 NUMEROS INVERSOS Y OPERACIONES INVERSAS.

Usaremos las propiedades básicas de las relaciones y operaciones estudiadas anteriormente para ampliar nuestro conjunto de números y sus operaciones, introduciendo los conceptos de "números inversos" y "operaciones inversas". El inverso de un número n debe considerarse en relación con una operación binaria (Cap. I - 2) tal como la adición o la multiplicación. Se dice que los números 2 y $\frac{1}{2}$ son inversos entre sí con respecto a la multiplicación, ya que $2 \cdot \frac{1}{2} = 1$ y 1 es el elemento de identidad para la multiplicación (Cap. I - 5). También, dado que $2 + (-2) = 0$, se dice que 2 y -2 son inversos con respecto a la adición. En general, se dice que dos números a, a' son *elementos inversos* con respecto a una operación arbitraria $\oplus$ con un elemento de identidad p si y sólo si $a \oplus a' = p$. El adjetivo "inverso" puede también aplicarse a operaciones binarias. Dos operaciones pueden denominarse operaciones inversas si su efecto es

opuesto, esto es, si al aplicarse sucesivamente al mismo número, el número original permanece invariable. Por ejemplo $(5 + 2) - 2 = 5$ y también $(5 \cdot 2) : 2 = 5$. En conformidad con esta definición se dirá que la sustracción es la operación inversa de la adición y que la división es la inversa de la multiplicación. En general, se dice que dos operaciones binarias $\oplus$ y $\ominus$ *son operaciones inversas* si y sólo si $(a \oplus b) \ominus b = a$, donde a y b son elementos cualesquiera de algún conjunto de elementos para el cual las operaciones estén definidas. Para definir la división emplearemos esta relación y la propiedad por la cual para $b \neq 0$ se verifica $ab = cb$ si y sólo si $a = c$ (Ejercicios 12 y 13, Cap. I - 5). Se escribe $a : b = c$ si y sólo si $a = bc$. De la misma manera, para la *sustracción* se escribe $a - b = c$ si y sólo si $a = b + c$ (ver Ejercicios 3 y 4, Cap. I - 5).

Las relaciones entre los números inversos y las operaciones inversas también serán útiles en el estudio de nuestro sistema de números. Por ejemplo, $5 - 2 = 5 + (-2)$ y $5 \div 2 = 5 \cdot (1/2)$. En general, tenemos la relación $b \oplus a = b \ominus a'$ si dado cualquier elemento b y elementos inversos a y a' con respecto a una operación arbitraria $\oplus$ con inversa $\ominus$ siempre que ambas operaciones estén definidas para los elementos dados.

Ya hemos introducido las cuatro operaciones racionales, adición, sustracción, multiplicación y división. La adición y la multiplicación se rigen por las propiedades que se han determinado en el Cap. I - 5; la sustracción y la división (excluyendo la división por cero) se han definido como las inversas de la adición y la multiplicación, respectivamente. Podemos también considerar una forma abreviada de la multiplicación repetida, a saber, la *potenciación* (la elevación de una cantidad a una potencia dada), junto con su operación inversa, la *radicación* (extracción de raíz). De estas operaciones surge la necesidad de definir nuevos símbolos como números, es decir, de ampliar gradualmente el conjunto de los elementos en estudio. El conjunto de los enteros positivos es cerrado para la adición, para la multiplicación y con respecto a la potenciación. Al considerar la división se necesitan los números racionales positivos; los números racionales positivos y negativos y cero, al considerar la división y la sustracción. Para tratar la radicación se necesita un conjunto aún más amplio de números. La adición, la sustracción, la multiplicación, la división, la potenciación y la radi-

cación pueden definirse para los números enteros positivos en el conjunto de los números reales. Estudiaremos el conjunto de números complejos con el objeto de obtener un conjunto de números tales que estas seis operaciones puedan ser definidas para todos los elementos diferentes de cero del conjunto (en lugar de serlo solamente para los números enteros positivos).

Después de haber alcanzado esta visión panorámica de nuestro sistema de números, consideraremos nuevamente el conjunto de los números enteros positivos. El conjunto de los números enteros positivos es cerrado para la suma y para la multiplicación. No es cerrado para la sustracción ni para la división. Desde el punto de vista práctico los enteros positivos sirven para contar objetos o para comparar conjuntos finitos de objetos. Aún no hemos mencionado números que sirvan para representar cosas tales como, por ejemplo, la porción que una persona recibe cuando se dividen tres manzanas en partes iguales entre seis personas, o la temperatura relativa a la cual se congela el agua. Por lo tanto hay que ampliar el conjunto de los números incluyendo en él a las fracciones (Cap. 1 - 8) y a los números orientados, es decir, precedidos de los signos $+$, $-$ (Cap. 1 - 9). En otras palabras, se necesitan números inversos para los números enteros positivos con respecto a la multiplicación y a la adición, junto con números que representen sumas de estos nuevos números.

EJERCICIOS

Demostrar cada uno de los siguientes ejercicios con respecto a los números enteros no negativos q, r, s, t elegidos arbitrariamente:

1. $r < s < t$ implica $t - s < t - r$.
2. $r < s < t$ implica $s - r < t - r$.
3. $q < r < s < t$ implica $s - r < t - q$.

1-8 LOS NUMEROS RACIONALES POSITIVOS.

El número inverso del número entero positivo b con respecto a la multiplicación se define como un número b' tal que satisfaga la relación $bb' = 1$. Se dice que $b' = 1/b$ es la *solución o raíz* de la ecuación $bx = 1$. También se llama *el cero* del polinomio $bx - 1$. Definiremos, ahora, un conjunto nuevo de números, los *números racionales positivos,* a fin de que podamos

resolver ecuaciones de la forma $bx = a$ para cualquier entero positivo a y b. Estos números pueden representarse por pares a/b de enteros positivos y tienen las siguientes propiedades:

(i) $\dfrac{a}{b} = \dfrac{c}{d}$ si y sólo si $ad = bc$;

(ii) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$;

(iii) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$; y

(iv) $\dfrac{a}{b} < \dfrac{c}{d}$ si y sólo si $abd^2 < b^2cd$.

La condición $abd^2 < b^2cd$ en (iv) se puede enunciar en la forma $ad < bc$ todas las veces que bd sea positivo. La forma $abd^2 < b^2cd$ se usa aquí dado que permanecerá válida cuando ampliemos el conjunto de números (Cap. I - 3) incluyendo en él a los números negativos.

Los números racionales positivos de la forma $a/1$ se identifican con los números enteros a. Técnicamente, el conjunto de enteros positivos es *isomorfo* con respecto al conjunto de los números racionales positivos de la forma $a/1$, es decir, existe una correspondencia biunívoca entre $a/1$ y a que se conserva en la adición y en la multiplicación. [$a/1 + b/1$ corresponde a $a + b$ y $(a/1)(b/1)$ corresponde a ab]. Este isomorfismo particular se mantiene también con respecto a las relaciones de orden (dado que $a/1 < b/1$ si y sólo si $a < b$) y se llama *isomorfismo de orden.*

Se dice que los pares iguales de enteros tales como los que se especifican en (i) anteriormente, representan el mismo número racional. En el conjunto de todos los pares de enteros que son iguales a un par dado, existe un par, digamos a/b tal que si r/s es cualquier otro par del conjunto, resulta $r = ta$ y $s = tb$ para algún

entero positivo t. Puede hacerse una demostración rigurosa de la existencia del par a/b (Ejercicio 16), valiéndose del hecho de que el conjunto de enteros positivos es bien ordenado (Ejercicio 6, Cap. 1-6). Se dice que el par a/b es la *forma reducida* del número racional dado.

Las definiciones anteriores permiten demostrar que para los números racionales positivos, la adición es única, asociativa, y conmutativa y que la multiplicación es única, asociativa, conmutativa, y satisface la ley de distributividad, es decir, la adición y la multiplicación tienen las mismas propiedades básicas (Cap. 1-5) en el conjunto de los números racionales positivos que en el conjunto de los enteros positivos. Por ejemplo, la suma anterior de (ii) es única, dado que $ad + bc$ y bd son únicos para enteros positivos cualesquiera a, b, c, d. De la misma manera, de

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b},$$

resulta que la adición es conmutativa. Las demostraciones restantes se dan como ejercicios al final de esta sección.

Si e y f son números racionales positivos, entonces tal como en el caso de los enteros positivos, $e - f = g$ se define como un número racional positivo si y sólo si existe un número racional positivo g tal que $e = f + g$. Análogamente, $e/f = h$, se define como un número racional positivo si y sólo si existe un número racional positivo h tal que $e = fh$. El número g existe si y sólo si $f < e$ [ver Ejercicio 5 (a)]; el número h existe siempre (Ejercicio 6). Por consiguiente, los pares e/f de números racionales positivos son a su vez ellos mismos números racionales y nada nuevo puede obtenerse al considerar estos pares de números racionales en vez de pares de números enteros. La propiedad [Ejercicio 5 (b)] de que para dos números racionales cualesquiera e, f, que satisfagan la relación $e < f$, existe un número racional positivo r que cumple con la relación $e < r < f$, se indica diciendo que los números racionales positivos son *densos*, es decir, que entre dos números racionales positivos distintos cualesquiera existe un tercer número racional positivo. Los enteros positivos no son densos.

Ya se ha definido el símbolo a^b (Cap. 1-5) para el caso de que a y b sean números enteros no negativos y por lo menos uno de

ellos sea diferente de cero. El símbolo r^b donde r es cualquier número racional positivo y b es cualquier número entero no negativo puede definirse exactamente como en el caso de los enteros, es decir, $r^0 = 1$ y r^b para cualquier entero positivo b indica el producto de b factores r. Ahora especificaremos que el símbolo $r^{1/b}$ en donde r es cualquier número racional positivo y b es cualquier entero positivo, debe satisfacer la relación $(r^{1/b})^b = r$, es decir, el producto de b factores $r^{1/b}$ debe ser igual a r. De este modo se conservará la propiedad $a^b a^c = a^{b+c}$ para los nuevos símbolos. El símbolo $r^{d/b}$ donde $r > 0$, indica el producto de d factores $r^{1/b}$, y el producto $r^s r^t$ se expresa por el símbolo r^{s+t} para números racionales positivos cualesquiera. Si s no es un entero, los nuevos símbolos r^s pueden no ser números racionales y las relaciones entre ellos aún no se han definido formalmente.

Las soluciones de las ecuaciones $x = a + b$, $x = ab$, y $ax = b$ son números racionales positivos para números racionales positivos a, b, cualesquiera, es decir, el conjunto de números racionales positivos es cerrado con respecto a la adición, a la multiplicación y a la división. Hemos ampliado nuestro concepto de número para incluir $a + b$, ab, y a/b en donde a, b son enteros positivos cualesquiera o números racionales positivos arbitrarios. Ampliaremos en seguida nuestro concepto de número y definiremos nuevos símbolos como números considerando la expresión $a - b$ para los casos en que a, b sean números racionales positivos arbitrarios o cero, es decir, sean *números racionales no negativos.*

EJERCICIOS

1. Demostrar que la adición de números racionales positivos es asociativa.
2. Demostrar que la multiplicación de números racionales positivos es (a) única, (b) asociativa, (c) conmutativa, y (d) distributiva con respecto a la adición.
3. Demostrar que $ac/bc = a/b$, siendo a, b, c enteros positivos elegidos arbitrariamente.
4. Demostrar que $(a + c)/b = a/b + c/b$, en donde a, b, c son enteros positivos arbitrarios.
5. Demostrar que si $a/b < c/d$ en donde a, b, c, d son enteros positivos arbitrarios, entonces existe (a) un número positivo racional g tal que $a/b + g = c/d$; y (b) un número positivo racional r tal que $a/b < r < c/d$.
6. Dados números enteros positivos cualesquiera a, b, c, d, demostrar que existe un número racional positivo h tal que $a/b = (c/d) \cdot h$.

7. Determinar que la *media aritmética o promedio* de dos números racionales positivos cualesquiera a, b es $m = (a + b)/2$, y en el caso en que $a < b$, demostrar que $a < m < b$.

8. Definir la expresión $0/1 = 0$ basándose en la suposición de que las propiedades (i) a (iv) enunciadas anteriormente son válidas para pares de números enteros no negativos a/b, $b \neq 0$, y demostrar que $0 < r$ siendo r cualquier número racional positivo.

9. Demostrar que $a < b$ implica $1/b < 1/a$, en donde a, b son (a) cualquier entero positivo; (b) cualquier número racional positivo.

10. Demostrar que $a < b$ y $c < d$ implica $a/d < b/c$ en donde a, b, c, d son (a) enteros positivos cualesquiera, (b) números racionales positivos cualesquiera.

11. Demostrar que a/b y b/a son números inversos con respecto a la multiplicación para números enteros positivos a, b arbitrarios.

12. Encontrar los números inversos con respecto a la multiplicación, siempre que tales números existan para cada uno de los números siguientes: 3, 5, 1/10, 1, 0, 10, 200.

13. Discutir, empleando ejemplos, qué conjuntos de números se necesitan para (a) resolver ecuaciones lineales y cuadráticas; (b) para efectuar las seis operaciones descritas en el Cap. I — 7.

14. Demostrar que los números racionales positivos están ordenados linealmente (Cap. I — 6).

15. Volver a formular las once propiedades de la relación $<$ que aparecen en el Cap. I — 6 de modo de obtener las once propiedades de esta misma relación $<$ para el caso en que a, b, c, d sean números racionales no negativos.

16. Demostrar que todo número racional positivo puede expresarse en forma reducida*.

I - 9 LOS NUMEROS NEGATIVOS.

Acabamos de considerar como símbolos pares a/b de números enteros positivos: hemos definido la igualdad, la adición, y la multiplicación de estos símbolos; hemos demostrado que estas definiciones son consistentes con las definiciones anteriores aplicadas a un subconjunto de elementos $a/1$ isomorfo con el conjunto original de elementos a, y hemos obtenido nuevos números (los números racionales positivos) al aceptar todos los símbolos a/b como números en que a y b son enteros positivos. Repetiremos ahora este proceso considerando como símbolos pares $[a - b]$ de números racionales no negativos, definiendo la igualdad, la suma y la multiplica-

*Ver definición en páginas anteriores. (N. de la T.).

ción de estos nuevos símbolos, demostrando que el conjunto de símbolos $[a - 0]$ es isomorfo con el conjunto de números no negativos a de acuerdo con estas nuevas definiciones y aceptando luego, todos los pares de números racionales no negativos $[a - b]$ como números racionales: positivos, negativos y cero.

Se definirá primero las relaciones y operaciones siguientes respecto a estos nuevos símbolos donde a, b, c, d son números racionales no negativos arbitrarios:

(i) $[a - b] = [c - d]$ si y sólo si $a + d = b + c$;
(ii) $[a - b] + [c - d] = [(a + c) - (b + d)]$;
(iii) $[a - b] \cdot [c - d] = [(ac + bd) - (bc + ad)]$;
(iv) $[a - b] < [c - d]$ si y sólo si $a + d < b + c$.

Tal como se ha hecho anteriormente, hemos definido el significado de las relaciones básicas $=$, $<$, y de las operaciones básicas $+$, $\cdot$ con respecto a los nuevos símbolos $[a - b]$. Demostraremos, ahora que la correspondencia entre $[a - 0]$ y a es un isomorfismo de orden (Cap. 1-8) y que las operaciones básicas tienen sus propiedades usuales en el conjunto completo de los pares de números $[a - b]$.

La correspondencia entre $[a - 0]$ y a es claramente biunívoca. Queda por demostrar que esta correspondencia subsiste respecto de la adición, de la multiplicación y en las relaciones de orden. Estas correspondencias pueden verificarse fácilmente dado que, por definición.

$$[a - 0] + [b - 0] = [(a + b) - (0 + 0)];$$
$$[a - 0] \cdot [b - 0] = [(ab + 0) - (0 + 0)];$$
$$[a - 0] < [b - 0] \text{ si y sólo si } a + 0 < b + 0.$$

Por consiguiente, el conjunto de las expresiones $[a - 0]$ donde a es un número racional no negativo es equivalente en el sentido de que es isomorfo con el conjunto de los números racionales no negativos.

Sean a, b en la expresión $[a - b]$ números racionales no negativos cualesquiera. Como en el caso de los números racionales positivos a/b, podemos probar que la suma de las expresiones $[a - b]$ es única, asociativa y conmutativa (Ejercicio 1), y que la multi-

plicación es única, asociativa, conmutativa y satisface la ley de distributividad (Ejercicio 2). En efecto, consideraremos todas las expresiones de la forma $[a - b]$ como números, *números racionales precedidos de signo,* en que a, b son números racionales no negativos arbitrarios. De acuerdo con el isomorfismo ya mencionado el número racional precedido de signo $[a - b]$ corresponde a 0 cuando $a = b$ y corresponde a d, cuando $a > b$ y $a = b + d$. Dado que una de las relaciones $a < b$, $a = b$, $a > b$, debe ser válida exactamente (Ejercicio, 4, Cap. 1-6 y Ejercicio 14, Cap. 1-8), necesitamos una expresión correspondiente análoga para $[a - b] = [0 - c]$ en donde $a < b$ y $a + c = b$. De consiguiente, definiremos ahora la expresión $[0 - c]$ como un *número racional negativo* y la expresión $[0 - c]$ la escribiremos $-c$. El número racional positivo c se denomina *valor numérico* o *valor absoluto* de $-c$ y de c, $c = |-c| = |c|$. Los números racionales positivos y negativos y el cero constituyen los números racionales precedidos de signo o simplemente los *números racionales.* Cuando a, b, son enteros positivos o cero, los pares $[a - b]$ pueden usarse de la misma manera que se hizo anteriormente para definir a los *enteros negativos.* Los números enteros positivos y negativos y el cero constituyen los *números enteros.*

Ya se ha definido la suma y la multiplicación para todos los números racionales. Se definirá ahora la sustracción y la división. La sustracción puede ser definida para números racionales arbitrarios por medio de la relación

$$[a - b] - [c - d] = [(a + d) - (b + c)]$$

(Ejercicio 3). La división de los números racionales puede definirse por

$$\frac{[a - b]}{[c - d]} = \left[\frac{ac + ad}{c^2 - d^2} - \frac{bc + bd}{c^2 - d^2}\right]$$

donde $c \neq d$. La división es indefinida cuando $c = d$. (Ejercicios 4 y 5). Estas definiciones nos permiten demostrar que

(i) $-a < -b$ si y sólo si $b < a$;
(ii) $a + (-b) = a - b$;
(iii) $(-a)b = a(-b) = -ab$; y
(iv) $(-a)(-b) = ab$,

para todos los números racionales a, b, no negativos. Por ejemplo, $-a < -b$ es por definición lo mismo que $[0 - a] < [0 - b]$ y nuevamente por definición esto es válido si y sólo si $0 + b < 0 + a$, esto es, si $b < a$. En forma análoga $a + (-b) = [a - 0] + [0 - b] = [(a + 0) - (0 + b)] = [(a - 0) - (b - 0)] = [(a - b) + (0 - 0)] = a - b$. Las dos demostraciones restantes constituyen el Ejercicio 6. Las demostraciones ponen en evidencia que las propiedades anteriores de los números precedidos de signo son una consecuencia de las definiciones enunciadas hasta ahora.

Podremos ahora ampliar la notación exponencial incluyendo exponentes negativos. Se define a^b como en el Cap. I-8 para cualquier entero positivo b y para cualquier número racional a. También como anteriormente, $a^0 = 1$ para cualquier valor de $a \neq 0$. Para obtener una definición con respecto a los exponentes negativos es necesario que a^{-b} satisfaga la expresión $a^{-b}a^b = 1$ para cualquier entero b y para cualquier número racional a, excepto 0. De esta manera se conserva la propiedad $a^b a^c = a^{b+c}$ para todos los números racionales $a \neq 0$ y para todos los números enteros b, c. Aún no se ha definido explícitamente el símbolo a^b para valores no enteros de b. Se considerará este asunto en el Cap. I-12. El símbolo 0^b es indefinido cuando b es negativo o cero.

El conjunto de todos los números racionales es cerrado con respecto a la adición, a la sustracción, a la multiplicación y a la división (excluyendo la división por cero), es decir, la suma, la diferencia, el producto y el cuociente (divisor diferente de cero) de dos números racionales arbitrarios son números racionales. A mucha gente le interesan principalmente los números racionales. Probablemente ellos bastan para la mayoría de los proveedores, oficinistas y aún banqueros. No obstante, los números racionales tienen también limitaciones bien determinadas. Por ejemplo, la distancia expresada en pies desde el "home plate" hasta la segunda base en baseball, y el diámetro en pulgadas de una pelota de baseball de nueve pulgadas de circunferencia, no pueden formularse con exactitud en números racionales. Pueden expresarse aproximadamente en números racionales, y el error en la aproximación puede hacerse menor que el producido por cualquier número racional positivo dado (de antemano).

La necesidad de ampliar el conjunto de los números racionales puede expresarse también en magnitudes. Hemos definido conjun-

tos finitos y números cardinales finitos (Cap. 1-2). Definiremos, ahora, un número d como un *número finito* si y sólo si existe un entero positivo N tal que $-N < d < N$. Se dice que cualquiera magnitud, cualquiera cantidad, cualquier objeto, cualquiera expresión algebraica, etc., es finita si se puede representar por o representa a un número finito. Necesitamos y por eso estudiaremos un conjunto de números, el conjunto de los números reales, que sirve para comparar magnitudes de dos objetos finitos similares cualesquiera. Toda magnitud finita puede representarse mediante un número real.

EJERCICIOS

1. Demostrar que la adición de los números racionales precedidos de signo es única, asociativa y conmutativa.

2. Demostrar que la multiplicación de los números racionales precedidos de signo es única, asociativa, conmutativa, y satisface la ley de distributividad.

3. Demostrar que la sustracción de los números racionales puede definirse mediante $[a - b] - [c - d] = [(a + d) - (b + c)]$ haciendo ver que según esta definición la sustracción es la operación inversa de la adición.

4. Demostrar que en el conjunto de los números racionales positivos y negativos (con exclusión del cero) la división tal como se definió anteriormente es la operación inversa de la multiplicación.

5. Demostrar que la división por cero no puede definirse en el conjunto de los números racionales.

6. Demostrar las propiedades indicadas en los números (iii) y (ix) para los números racionales.

7. Demostrar que $-c < 0$ para cualquier número racional positivo c.

8. Demostrar que $a < b$ y $c < 0$ implican $bc < ac$.

9. Indicar cuales de los ejercicios del Cap. 1 — 7 pueden demostrarse cuando q, r, s, t son números racionales arbitrarios (positivos, negativos o cero).

10. Demostrar, por medio de la expresión $a^{-n} = 1/a^n$ que para enteros q, r, y para números racionales s, t las relaciones $q < r < 0$ y $0 < s < t < 1$ implican $1 < t^r$, $t^r < t^q$, y $t^r < s^q$.

11. Obtener el número inverso con respecto a la adición para cada uno de los siguientes números: 3, —5, 1/10, 1, 0, 10, —200.

12. Hacer una lista de los números racionales que son sus propios inversos con respecto a la suma y a la multiplicación.

13. Demostrar que $[a - b]$ y $[b - a]$ son inversos con respecto a la adición para numeros racionales positivos a, b arbitrarios.

14. Demostrar que los números racionales están ordenados línealmente.

15. Formular de nuevo las once propiedades de la relación $<$ del Cap. I — 6 con el objeto de obtener las onces propiedades para $<$ cuando a, b, c, d son números racionales.

I-10 LOS NUMEROS REALES.

El número asociado con un objeto o conjuntos de objetos representa comúnmente una medida o magnitud relativa a alguna unidad conocida, por ejemplo, la altura de un árbol en pies, la extensión de una hacienda en acres, o el número de manzanas de una caja (comparado con una manzana). Cuando la medida de un objeto en relación a otro no se puede expresar como un cuociente entre enteros, los dos objetos se llaman *inconmensurables.* Los griegos de la antigüedad observaron que la diagonal y el lado de un cuadrado son inconmensurables. La circunferencia y el diámetro de un círculo son también inconmensurables. Todo número que no pueda expresarse como cuociente entre dos enteros se llama *irracional.*

Probaremos ahora que $\sqrt{2}$ es irracional. Supongamos que $\sqrt{2} = a/b$, donde a y b son enteros que no tienen un factor común entero. Entonces $a^2 = 2b^2$, de aquí que resulte que a^2 es un entero par. Por lo tanto, dado que sólo un entero par puede tener un entero par como su cuadrado, a es divisible por 2. Sea $a = 2c$. Entonces resulta $4c^2 = 2b^2$, $2c^2 = b^2$, y b es divisible por 2, contrariamente a nuestra suposición de que a y b no tienen factores comunes enteros. Por lo tanto la primera suposición de que $\sqrt{2} = a/b$ es imposible, y $\sqrt{2}$ es un número irracional.

El método de demostración anterior suele denominarse método de *demostración directa* o *reductio ad absurdum.* Consiste en suponer que la conclusión deseada es falsa y en valerse de esta suposición y de la hipótesis dada para efectuar una demostración lógica de alguna aserción que sea contraria a la suposición o la hipótesis. (Ejercicio 1). En seguida se dice que puesto que la suposición conduce a una contradicción, la suposición debe ser falsa, es decir la conclusión deseada debe ser verdadera. Una forma de demostración indirecta de un teorema, por ejemplo, *(A* implica *B)* es la demostración directa del teorema *contrarrecíproco* ("no *B*" implica "no *A*"). El método de demostración indirecta puede considerarse también como un caso especial de demostración por eliminación (Ejercicio 4).

Los números irracionales tales como $\sqrt{2}$ pueden definirse de varias maneras. Nos alejaremos momentáneamente de nuestro tratamiento sistemático del sistema de números con el objeto de examinar brevemente la notación decimal para representar a todos los números reales (racionales e irracionales). En realidad, las definiciones de y las operaciones con decimales infinitos se basan sobre los mismos conceptos fundamentales de sucesiones infinitas y límites (Cap. III-11). Por el momento nuestras consideraciones serán algo intuitivas. Las definiciones rigurosas se harán en la sección siguiente en función de las cortaduras de Dedekind. Todos los conceptos intuitivos que se usan en esta sección pueden probarse rigurosamente basándose en las definiciones sistemáticas.

En el Cap. II-6 demostraremos que cualquier entero positivo N puede expresarse en la "base" 10 en la forma

$$N = d_k\, 10^k + d_{k-1}\, 10^{k-1} + \ldots + d_2\, 10^2 + d_1\, 10 + d_0,$$

donde los d_i son elementos del conjunto 0, 1, 2, ..., 9 de *dígitos* de la base diez. Por ejemplo, 1953 significa $1 \cdot 10^3 + 9 \cdot 10^2 + 5 \cdot 10 + 3$. Ciertas fracciones pueden expresarse en la forma:

$$N + a_1/10 + a_2/10^2 + \ldots + a_m/10^m,$$

donde N y m son enteros positivos y los a_i son dígitos. Por ejemplo, $123/4 = 30 + 7/10 + 5/10^2 = 30.75$. Concretamente, un número racional $r = a/b$ puede representarse por medio de un número finito de términos como en la notación decimal precedente (es decir, por medio de *un decimal exacto*) si y sólo si r es un entero o bien si $10^m r$ puede expresarse como número entero para algún número entero positivo m. Dado que $2^0 = 5^0 = 1$, esta condición puede formularse como sigue: un número racional r puede expresarse como un decimal exacto si y sólo si existen enteros a, p, q tales que $r = a/(2^p 5^q)$.

Se debe aceptar que el símbolo 1.333 ... es un número con el objeto de poder expresar el número racional $4/3$ en notación decimal. En rigor, esto envuelve los conceptos de sucesiones infinitas y de límites. Decimales como el anterior o como $\frac{15}{7} = 2.142857142857$ ..., que consisten en conjuntos de dígitos, tal como el 3 en el caso

de $\frac{4}{3}$ y 142857 en el caso de $\frac{15}{7}$, repetidos indefinidamente se llaman *decimales periódicos infinitos.* También se puede considerar a los decimales exactos como decimales periódicos infinitos haciendo $a_j = 0$ para el valor j suficientemente grande. Por ejemplo, $0.25 = 0.2500000$ .... Demostraremos en el Cap. II-7 que todo número racional puede representarse como un decimal periódico infinito y, a la inversa, todo decimal periódico infinito, representa un número racional. Es fácil imaginarse la proposición conversa mediante el procedimiento siguiente: dado cualquier decimal periódico d en el que se repite indefinidamente un conjunto de k dígitos, calcular $10^k \cdot d - d$ y dividir por $10^k - 1$. Por ejemplo, si $d = 1.333...$, se calcula $10d - d = 13.333... - 1.333... = 12$, de donde $d = \frac{4}{3}$. Si d $= 0.164545...$, entonces $100d - d = 16.29$, de donde $d = 16.29/99 = 1629/9900$. Como se señaló anteriormente, una definición precisa de la sustracción de decimales infinitos requiere el concepto de límite.

Definiremos, ahora, un *decimal infinito* como la expresión:

$$N + a_1/10 + a_2/10^2 + ... + a_n/10^n + ...,$$

donde N es un entero y los a_j son dígitos. De las consideraciones anteriores se desprende que, una vez hechas las definiciones adecuadas, es posible demostrar que un subconjunto (los decimales periódicos infinitos) del conjunto de los decimales infinitos es isomorfo con el conjunto de los números racionales. En general, se puede definir la igualdad, la suma y el producto de decimales infinitos, de modo que todos los decimales infinitos se comportan como números. De esta manera, se puede representar números nuevos, *números irracionales,* tales como $\pi = 3.1415926536...$ (ver Bibliografía Nº 40, págs. 39-40), como *decimales infinitos no periódicos.* El conjunto de todos los decimales infinitos, es decir, el conjunto total de números racionales e irracionales, se llama el conjunto de los *números reales.* En consecuencia, si convenimos en que *todos los decimales infinitos representan números,* obtenemos el conjunto de los números reales. Dado que esta suposición, en último término, envuelve el concepto de límites de sucesiones infinitas, basaremos nuestro estudio sistemático del sistema de números reales sobre las cortaduras de Dedekind (Cap. I-11). Se ha se-

ñalado la Sección 11 del Cap. I como optativa para indicar que cualquier lector que desee aceptar las propiedades corrientes de los decimales infinitos sin una demostración rigurosa pueda prescindir de esa sección.

Los números reales pueden clasificarse de diversas maneras. Son positivos, negativos o cero. Son racionales o irracionales. Son algebraicos o trascendentes. Se dice que un número es *algebraico* si satisface alguna ecuación de la forma.

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0,\ a_0 \neq 0$$

donde los a son enteros y n es un entero positivo. De todos los demás números reales se dice que son *trascendentes*. Cualquier número racional a/b satisface la ecuación $bx - a = 0$, y, por lo tanto, es algebraico. Algunos números irracionales, como $\sqrt{2}$ que satisface la condición $x^2 - 2 = 0$, son algebraicos. También existen números algebraicos, tales como i y $-i$ que satisfacen la ecuación $x^2 + 1 = 0$, y que no son números reales. Un número algebraico real puede ser racional o irracional; todos los números reales trascendentes son irracionales. La base de los logaritmos naturales

$$e = \lim_{x \to 0} (1 + x)^{1/x}$$

es un número trascendente real; también lo es π, la razón entre la circunferencia y el diámetro de un círculo (ver Bibliografía Nº 29, págs. 71-89, 111). El símbolo πi, donde i satisface la ecuación $x^2 + 1 = 0$, representa un número trascendente que no es un número real.

EJERCICIOS

1. Dos proposiciones son *contrarias* si ambas no pueden ser verdaderas simultáneamente. Por ejemplo, las proposiciones "El automóvil es un Ford" y "El automóvil es un Dodge" son contrarias. Enunciar cinco pares de proposiciones contrarias.

2. Dos proposiciones son *contradictorias* si ambas no pueden ser verdaderas ni tampoco pueden ser ambas falsas. Las proporciones dadas en el ejemplo ilustrativo del Ejercicio 1, no son contradictorias, dado que ambas podrían ser falsas. Las proposiciones contradictorias son importantes, ya que si una es verdadera, la otra es falsa; y si una es falsa, la otra es verdadera. Formular cinco pares de juicios contradictorios.

3. Indicar cuáles de los pares de las proposiciones dadas en la respuesta al Ejercicio 1, son contradictorios.

4. El método de prueba por eliminación consiste en considerar todas las posibilidades y en eliminar todas ellas excepto una. Por ejemplo, si deseamos demostrar que el triángulo ABC es un triángulo isósceles rectángulo, habrá que considerar las siguientes posibilidades: (a) el triángulo ABC no es un triángulo rectángulo; (b) el triángulo ABC no es un triángulo isósceles; (c) el triángulo ABC es un triángulo isósceles rectángulo. Proponer otro ejemplo de esta clase de razonamiento.

5. Demostrar que $\sqrt{5}$ es un número irracional.

6. Expresar 1.41414 . . . en forma de número racional.

7. Expresar 3.176176176 . . . en forma de número racional.

8. Proponer cinco números racionales algebraicos.

9. Proponer cinco números irracionales algebraicos.

10. Dar ejemplos de tres números que el lector crea que son trascendentes (la demostración sistemática de que un número dado es trascendente puede ser muy difícil).

11. Indicar la relación entre la clasificación de los números reales en racionales e irracionales y la clasificación de los números reales en decimales exactos, infinitos periódicos o infinitos no periódicos.

12. Demostrar la necesidad de ampliar nuestro sistema de números reales, dando ejemplos de cinco números algebraicos que no sean números reales.

13. Hacer un cuadro indicando las relaciones entre los números reales, algebraicos, trascendentes, racionales, irracionales y enteros.

14. Encontrar ecuaciones (con coeficientes enteros) que se satisfagan con cada uno de los siguientes números:

(a) $3 + \sqrt{2}$ (c) $\sqrt{10 - 2\sqrt{5}}$

(b) $\sqrt{3 + \sqrt{2}}$ (d) $\sqrt[3]{4 - \sqrt[3]{2}}$

¿Tienen estos ejercicios una respuesta única? Explicar.

15. Demostrar que

$$(a + b\sqrt[3]{c - d})/e$$

es un número algebraico donde $a, b, c, d,$ y $e \neq 0$ son enteros.

I-11* LOS POSTULADOS DE LOS NUMEROS REALES.

Repetiremos, ahora, el procedimiento de definir operaciones y relaciones respecto de nuevos símbolos. Los nuevos símbolos se llamarán *cortaduras de Dedekind* o,

*El asterisco indica que esta sección (Cap. I - 11) puede omitirse sin perturbar la organización del texto.

simplemente, *cortaduras.* El postulado siguiente que se refiere a la existencia de números que corresponden a cortaduras, se denomina *postulado de Dedekind.*

Si dividimos el conjunto de todos los números racionales en dos subconjuntos L y R de tal manera que todo número racional pertenezca ya sea a L o a R, pero no a ambos, que ni L ni R sean conjuntos vacíos y que a perteneciente a L y b perteneciente a R impliquen la relación $a < b$, *existe, entonces, un número c cortadura tal que a perteneciente a L implica* $a \leqq c$ *y b perteneciente a R implica que* $c \leqq b$.

Este procedimiento para formar una cortadura puede aplicarse a cualquier conjunto de elementos en el cual se hayan definido las relaciones de orden. Nos referiremos principalmente a cortaduras $\{L, R\}$ en el conjunto de los números racionales. Si L comprende a todos los números racionales $x \leqq 3$, y R contiene todos los $x > 3$, entonces $c = 3$ y c pertenece a L. Si L contiene a todos los números $x < 5$ y R a todos $x \geqq 5$, entonces $c = 5$ y c se encuentra en R. Nótese que c es racional y en estos dos ejemplos pertenece a L o a R. Si L contiene a todos los números negativos x, y a todos los números no negativos x, tales que $x^2 < 2$, y si R contiene a todos los números positivos x tales que $x^2 > 2$, entonces todos los números racionales se encuentran en L o en R y $c = \sqrt{2}$ no pertenece ni a L ni a R (Cap. 1-10). En general, cuando los conjuntos L y R son subconjuntos del conjunto de los números racionales, el número cortadura c se encuentra en L o en R, si y sólo si c es racional. Se dice que una cortadura es *cerrada* si el número cortadura c es un elemento del conjunto y, en caso contrario, la cortadura es *abierta.* Por eso, una cortadura en el conjunto de los números racionales es cerrada si c es racional, y abierta si c es irracional, es decir, no racional. El conjunto de todos los números cortaduras que se obtienen de cortaduras en el conjunto de los números racionales, se llama el conjunto de los *números reales.* El resultado de efectuar una cortadura en el conjunto de los números reales se acostumbra a enunciarlo en forma de un teorema, el *Teorema de Dedekind: Toda cortadura en el sistema de números reales es cerrada* (Ejercicio 10).

Dadas dos cortaduras $\{L, R\}$ y $\{S, T\}$ en el conjunto de los números racionales, formularemos las siguientes definiciones:

(i) $\{L, R\} = \{S, T\}$ si hay, a lo sumo, un elemento de S que no es elemento de L y viceversa, si hay, a lo sumo, un elemento de L que no es elemento de S.

(ii) $\{L, R\} < \{S, T\}$, si hay, por lo menos, dos elementos de S que no son elementos de L.

(iii) $\{L, R\} + \{S, T\} = \{U, V\}$, en donde U comprende a todos los números racionales que puedan expresarse en la forma $a + s$, donde a pertenece a L y s pertenece a S.

Las expresiones "a lo sumo un elemento" en (i) y "por lo menos dos elementos" en (ii), son necesarias, puesto que la cortadura $\{L, R\}$ donde L comprende a todos los $x < 2$ y la cortadura $\{S, T\}$ donde S contiene a todos los $x \leqq 2$ tienen el mismo número cortadura $c = 2$ y deben considerarse iguales. Cada una de las definiciones anteriores puede expresarse también (Ejercicio 4) con respecto a las condiciones de R, T y V, ya que por definición de una cortadura $\{L, R\}$ en el conjunto de los números racionales, todo número racional debe pertenecer a L o a R, de donde R contiene a todos los números racionales que no pertenecen a L.

La cortadura $\{N, P\}$ en la que todos los números racionales negativos y cero se encuentran en N y todos los números racionales positivos pertenecen a P, se denomina *cortadura cero*. Se dice que una cortadura $\{L, R\}$ es *negativa* si $\{L, R\} < \{N, P\}$; es *cero* si $\{L, R\} = \{N, P\}$ y es *positiva* si $\{N, P\} < \{L, R\}$. Una cortadura que es positiva o cero se dice que es *no negativa*. El producto de dos cortaduras $\{L, R\} \cdot \{S, T\} = \{U, V\}$ puede definirse considerando los casos posibles de cortaduras negativas y no negativas. Definiremos a V como el conjunto de números racionales que se pueden expresar en la forma as, donde a pertenece a L, y s pertenece a S, cuando las dos cortaduras dadas son negativas; y cuando las dos cortaduras dadas son no negativas, definiremos a V como el conjunto de números racionales que se expresa en la forma rt, donde r pertenece a R y t pertenece a T. Si una de las cortaduras dadas es no negativa y la otra es negativa, U comprende al conjunto de los números racionales que se expresan en la forma at, donde a pertenece a L y t pertenece a T, cuando $\{L, R\}$ es negativa; y cuando $\{S, T\}$ es negativa, U comprende al conjunto de los números racionales susceptibles de expresarse en la forma sr, donde s pertenece a S y r pertenece a R.

Ya hemos definido la igualdad, las relaciones de orden, la suma y la multiplicación para los nuevos símbolos $\{L, R\}$. Como en el caso de los símbolos a/b y $[a - b]$, queda por demostrar que existe un isomorfismo de orden entre un subconjunto de los nuevos símbolos y el conjunto dado de números, o sea, el conjunto de los números racionales. Consideraremos la correspondencia de $\{L, R\}$ con c, donde c es un número racional y L contiene a todos los números racionales $x \leqq c$. Esto es, en esencia, la correspondencia entre cortaduras cerradas y los números racionales, ya que V comprende a todos los números racionales $\leqq c$, luego $\{U, V\} = \{L, R\}$.

Dadas dos cortaduras $\{L, R\}$, $\{S, T\}$, que correspondan a números racionales a y b, respectivamente, las definiciones anteriores pueden aprovecharse para demostrar que $\{L, R\} = \{S, T\}$ si y sólo si $a = b$; que $\{L, R\} < \{S, T\}$, si y sólo si $a < b$; que $\{L, R\} + \{S, T\}$ corresponde a $a + b$; y que $\{L, R\} \cdot \{S, T\}$ corresponde a $a \cdot b$. Las demostraciones no son difíciles y se han dejado como ejercicio para el lector (Ejercicio 7). El isomorfismo de orden entre el conjunto de cortaduras cerradas y el conjunto de números racionales, muestra que para el conjunto de cortaduras cerradas, las definiciones anteriores son consistentes con nuestras definiciones previas. Tal como se señaló anteriormente, los números cortaduras representados por los nuevos símbolos se llaman números reales para cortaduras arbitrarias $\{L, R\}$ pertenecientes al conjunto de los números racionales. De esta manera, hemos obtenido números nuevos, *los números irracionales* que son los que corresponden a cortaduras abiertas. El Postulado de Dedekind sobre la existencia de un número cortadura c para todas las cortaduras pertenecientes al conjunto de los números racionales, sirve para postular la existencia de todos los números reales, racionales e irracionales en relación con los números racionales. El Teorema de Dedekind (todas las cortaduras en el conjunto de los números reales son cerradas) puede probarse (Ejercicio 10) demostrando que todas las cortaduras en el conjunto de los números reales determinan una cortadura en el conjunto de los números racionales. Varias otras propiedades de las cortaduras de Dedekind y de los números reales se tratarán en los ejercicios siguientes y en el Cap. 1-12.

EJERCICIOS

1. Citar dos ejemplos de cortaduras abiertas en el conjunto de números racionales.

2. Citar dos ejemplos de cortaduras cerradas en el conjunto de los números racionales.

3. Demostrar que toda cortadura en el conjunto de los números enteros es cerrada.

4. Formular de nuevo las definiciones anteriores (i) (ii) y (iii) con respecto a R, T, y V.

5. Proponer una cortadura cero $\{N', P'\} = \{N, P\}$ tal que los conjuntos N' y N sean diferentes.

6. Construir la cortadura que sea la suma de las dos cortaduras dadas en la respuesta del Ejercicio 1.

7. Dadas dos cortaduras cerradas $\{L, R\}$, $\{S, T\}$ correspondientes a a y b respectivamente, demostrar que $\{L, R\} = \{S, T\}$ si y sólo si $a = b$; $\{L, R\} < \{S, T\}$ si y sólo si $a < b$; $\{L, R\} + \{S, T\}$ corresponde a $a + b$; y $\{L, R\} \cdot \{S, T\}$ corresponde a $a \cdot b$.

8. Repetir el Ejercicio 6 respecto del producto.

9. Definir la sustracción de las cortaduras y repetir el Ejercicio 6 respecto de la sustracción.

10. Demostrar el Teorema de Dedekind.

11. Definir la división de una cortadura arbitraria por una cortadura diferente de cero. Dar un ejemplo numérico.

12. Demostrar que los números reales están ordenados linealmente (Cap. 1 — 6).

13. Demostrar que los números reales son densos (Cap. 1 — 8).

I-12 PROPIEDADES DE LOS NUMEROS REALES. Acabamos de aceptar que los números reales existen y están ordenados linealmente (Ejercicio 12, Cap. I-11). Se los puede considerar ya sea como decimales (Cap. I-10) o bien como cortaduras de Dedekind (Cap. I-11). También damos por aceptado que se han definido las cuatros operaciones racionales y que tienen las mismas propiedades en el conjunto de los números reales que en el conjunto de los números racionales (Cap. I-11).

Dado cualquier número real a y cualquier entero positivo b, determinaremos que el símbolo a^b representa el producto de b factores a. Si $a \neq 0$, definiremos $a^0 = 1$ y $a^{-b}\, a^b = 1$ para cualquier entero b. Si $a = 0$ y b es cualquier número real positivo, entonces

$a^b = 0$. Definiremos $(a^{1/b})^b = a$ para cualquier número racional b cuando $a > 0$, y para cualquier entero impar b cuando $a < 0$. Estas definiciones permiten conservar la propiedad $a^b\ a^c = a^{b+c}$ siempre que los símbolos estén definidos. En general, para cualquier número real a y para cualquier número racional b, por ejemplo, $b = r/s$ donde los enteros r, s no tienen factores comunes, el símbolo a^b representa un número real si y sólo si el entero r puede elegirse de modo que a^r esté definido y que la ecuación $x^s = a^r$ tenga una solución en el conjunto de los números reales. Este concepto puede aplicarse (Ejercicios 10, 11, 12 y 13) a los números reales a con el objeto de dar un significado preciso al símbolo a^b en el conjunto de los números reales sujetos a cualquiera de las siguientes condiciones:

(i) $a = 0$ y b es cualquier número positivo real;
(ii) $a > 0$ y b es cualquier número real, y
(iii) $a < 0$ y $b = r/s$ donde los enteros r, s no tienen factores comunes y s es número impar (no tiene factor 2).

Cuando $a = 0$ y $b \leq 0$, no se le puede atribuir al símbolo a^b un significado explícito dentro del conjunto de los números reales y conservar, al mismo tiempo, la propiedad $a^b\ a^c = a^{b+c}$. Cuando $a < 0$ y b es irracional, o $b = r/s$, donde r y s no tienen factores comunes y s es par, el símbolo a^b no tiene un significado explícito en el conjunto de los números reales, pero puede definirse en el conjunto de los números complejos (Cap. I-16).

Todas las propiedades del conjunto de los números reales pueden considerarse también como propiedades del conjunto de puntos de una recta. Supondremos que el lector está familiarizado con el uso de un sistema de coordenadas cartesianas ortogonales en la geometría plana de Euclides. En cualquier sistema dado de coordenadas, como el ya citado, definiremos los puntos que tienen números enteros por coordenadas, como *puntos enteros;* definiremos como *puntos racionales* a los que tienen números racionales por coordenadas y como *puntos reales* a aquéllos que tienen por coordenadas, números reales. Dado un origen y un punto unidad, todos los puntos enteros y racionales pueden construirse con regla y compás (Cap. VI-4). También, pueden construirse algunos puntos irracionales, como $\sqrt{2}$, la diagonal de un cuadrado, cuyo lado es la unidad. La existencia del conjunto de los puntos irra-

cionales debe postularse. Euclides supuso que cualquier segmento de recta que uniera el centro de un círculo con un punto fuera del círculo, contenía un punto del círculo. Nosotros admitiremos el Axioma de *Cantor-Dedekind:*

A cada punto de una recta corresponde uno y sólo un número real e inversamente, a cada número real corresponde uno y sólo un punto de una recta.

Esta correspondencia biunívoca puede elegirse, como en el caso de los sistemas de coordenadas corrientes de modo que exista un isomorfismo de orden entre el conjunto de los puntos de la línea recta y el conjunto de los números reales. Esta correspondencia, pues, hace posible obtener una representación geométrica de las propiedades del conjunto de los números reales. Por ejemplo, los números reales y racionales son densos (Cap. 1-8); los enteros no son densos. Todos los números enteros, racionales y reales están ordenados linealmente (Cap. 1-6).

La propiedad que distingue al conjunto de los números racionales del conjunto de los números reales es la continuidad. Esta es la propiedad que se utiliza en geometría plana para demostrar que cualquiera recta que una el centro de un círculo con un punto fuera de él, debe cortar al círculo, por lo menos en un punto. Intuitivamente, una línea recta o curva es continua si no "se rompe" o "interrumpe". Técnicamente, valiéndonos del Axioma de Cantor-Dedekind, representaremos los elementos de cualquier conjunto dado ordenado linealmente como un conjunto ordenado de puntos de una recta, y consideraremos a los números reales (coordenadas) asociados con estos puntos. Definiremos entonces el conjunto de elementos dado ordenado linealmente y el conjunto de puntos asociado con él como *continuos* si y sólo si el conjunto correspondiente de números reales incluye a todos los números reales x o comprende a todos los números reales x que satisfacen alguna de las relaciones $a < x$, $x < b$, $a < x < b$ para algunos números reales a, b. Esta definición puede formularse en forma mucho más elegante empleando la terminología del Cap. 1-11. Se dice que un conjunto de elementos linealmente ordenados, es continuo, si es denso y satisface el Postulado de Dedekind. Es así como los números racionales son densos, pero no continuos; los números rea-

les son densos y continuos. Las definiciones anteriores de conjuntos densos y continuos pueden ampliarse a conjuntos de puntos en un plano y a muchos otros conjuntos que no pueden ser ordenados linealmente.

Las proposiciones contenidas en el Ejercicio 9 señalan, principalmente, métodos para ampliar un conjunto denso, ordenado linealmente y convertirlo en un conjunto continuo. Por ejemplo, cada uno de los números.

$$1,\ 1.4,\ 1.41,\ 1.414,\ 1.4142,\ 1.41421,\ 1.414214,\ \ldots$$

puede expresarse en forma de un número racional que tenga por denominador una potencia de diez (Cap. I-10). Sin embargo, si consideramos una sucesión tal de números x_1, x_2, x_3, ..., que satisfaga,

$$2 - x_1^2 > 2 - x_2^2 > 2 - x_3^2 > \ldots,$$

y tal que para cualquier número e *racional* positivo dado, el número positivo $2 - x_n^2$ pueda hacerse menor que e eligiendo n suficientemente grande, es decir, haciendo aproximaciones más y más próximas a $\sqrt{2}$, entonces esta sucesión sin fin de números puede decirse que define un nuevo número $\sqrt{2}$. En la terminología del análisis algebraico, la sucesión anterior de números racionales tiene a $\sqrt{2}$ como límite (Cap. III-11). En general, cualquier conjunto de elementos denso ordenado linealmente puede hacerse continuo agregando todos los límites de las sucesiones convergentes de sus elementos (Cap. III-11). Por ejemplo, el conjunto de los números racionales se convirtió en un conjunto continuo (el conjunto de los números reales) al agregar los números irracionales. Todo número irracional puede expresarse como límite de una sucesión de números racionales.

La última propiedad de los números reales que consideraremos es la propiedad de tener límites. La palabra "límite" se usa frecuentemente para indicar un ámbito que no puede o no debe excederse. La frase "fuera de los límites" es corriente en muchos juegos. Todo objeto físico tiene límites. Las inmensas regiones polares despobladas de la Antártica están limitadas por océanos. El aire

que respiramos es una parte de la atmósfera de la tierra que está limitada, dado que no se extiende hasta el sol, hasta otro planeta, ni aún hasta la luna. El número de pelos de la cabeza de una persona y el número de granos de arena de la playa de Miami son limitados, aun cuando, por lo menos, en el segundo caso, el número es grande.

La palabra "ilimitado" se usa para indicar que un objeto o los elementos de un conjunto exceden cualquier límite que se pretenda establecer para él. Se dice que el conjunto de enteros positivos es ilimitado, ya que si se considera cualquier número real M como límite, siempre existe un número entero n tal que $n > M$. Para ser más exactos, decimos que los enteros positivos tienen un límite inferior que es cero, o cualquier número negativo y que en su extremo superior son ilimitados. Lo mismo puede decirse de los números reales positivos. Los enteros negativos son ilimitados en su extremo inferior y son limitados en su extremo superior. El conjunto de todos los enteros es ilimitado en sus extremos inferior y superior, es decir, es *ilimitado*. Análogamente, los números reales son ilimitados.

El conjunto de los números reales positivos $\leqq N$ está limitado por 0 y por N. Cualquier conjunto numerado de números reales está limitado. Por ejemplo, el conjunto 1, 5, 75, 32, 17, -4 está limitado por -4 y 75 o por -10 y 100, ... En efecto, los límites no son únicos y cualquier número real determinado está limitado. Por ejemplo, cualquier número real n está limitado por $n - 1$ y $n + 1$. Cada uno de los números reales, considerados individualmente, está limitado, pero el conjunto de todos los números reales es ilimitado. Lo mismo puede decirse del conjunto de números enteros. Se dice que un conjunto de números reales está *limitado* si existe un número entero positivo fijo N tal que $-N < b < N$ para todos los elementos b del conjunto. En la sección siguiente de este capítulo consideraremos conjuntos ilimitados de elementos y nos referiremos, particularmente, a los conjuntos de elementos que puedan ordenarse en correspondencia biunívoca con respecto al conjunto de los números enteros positivos.

EJERCICIOS

1. Indicar cuáles de los siguientes conjuntos de elementos son linealmente ordenados: (a) los números enteros; (b) los números racionales; (c) los nú-

meros irracionales; (d) los números reales algebraicos; (e) los puntos de un círculo en la geometría de Euclides, y (f) los puntos de un segmento de recta limitado en la geometría de Euclides.

2. Señalar cuáles de los conjuntos de elementos del Ejercicio 1 son densos.

3. Indicar cuáles de los conjuntos de elementos del Ejercicio 1 son continuos.

4. Demostrar que todo conjunto continuo linealmente ordenado, debe ser también denso.

5. Indicar una propiedad del conjunto de los números reales que lo distinga del conjunto de los números racionales.

6. Indicar una propiedad del conjunto de los números racionales que lo distinga del conjunto de los números enteros.

7. Citar tres conjuntos de números que posean las siguientes propiedades: (a) tener límite inferior y superior; (b) tener límite inferior solamente; (c) tener límite superior solamente; (d) ser ilimitados; (e) ser limitados.

8. Citar dos conjuntos de límites, en el caso de que exista alguno, para cada uno de los conjuntos de números dados en las respuestas al Ejercicio 7.

9. Dar ejemplos algebraicos o geométricos de cada una de las siguientes proposiciones. Cada proposición puede servir para postular la existencia del conjunto de números reales y, en este sentido, es equivalente al Postulado de Dedekind. Cualquiera de estas proposiciones puede considerarse también como base suficiente para probar la continuidad tanto en álgebra como en geometría.

a) Toda fracción decimal está dada como un número real.

b) *Teorema de Bolzano Weierstrass:* Todo conjunto acotado de infinitos puntos admite por lo menos un punto límite.

c) Todo conjunto de puntos acotado en su extremo inferior tiene una cota inferior máxima.

d) Todo conjunto de puntos acotado en su extremo superior tiene una cota superior mínima.

e) *Teorema de Heine - Borel - Lebesgue:* Si un conjunto infinito de intervalos I comprende un conjunto fundamental de puntos S en un intervalo cerrado finito, entonces, existe un subconjunto finito de I que comprende a S.

f) Toda sucesión de Cauchy de números racionales determina un número real (Cap. III-11).

g) *Teorema de Cantor:* Dada una sucesión cualquiera de intervalos E_1, E_2, E_3, ... sobre una recta, en que E_i está determinado por $a_i \leqq x \leqq b_i$ y en donde se verifican las relaciones $a_1 \leqq a_2 \leqq a_3 \leqq \dots, \dots \leqq b_3 \leqq b_2 \leqq b_1$, entonces existe por lo menos un punto, sea $x = x_0$, que pertenece a todos los intervalos de la sucesión.

10. Definir a^b para cualquier número real $a \neq 0$ y para cualquier entero b.

*11. Definir a^b como un número positivo para cualquier número real positivo a y cualquier número real b.

12. Definir a^b para cualquier número real negativo a y cualquier número racional $b = r/s$, donde los enteros r, s no tengan factores comunes y s sea impar.

13. Demostrar que a^b está determinado unívocamente por las condiciones expuestas en los Ejercicios 10, 11, 12.

I-13 LOS NUMEROS CARDINALES TRANSFINITOS. En las secciones 1 y 2 del Cap. I se han considerado los números cardinales asociados con conjuntos finitos de elementos. Dos conjuntos finitos tienen el mismo número cardinal si y sólo si existe una correspondencia biunívoca entre los elementos de los dos conjuntos. Ahora, mediante correspondencias biunívocas, asociaremos números cardinales (*números cardinales transfinitos*) con conjuntos infinitos (Cap. I-2).

Dos conjuntos infinitos de elementos tienen el mismo número cardinal transfinito si y sólo si existe una correspondencia biunívoca entre los elementos de los dos conjuntos. Como en el caso de los conjuntos finitos, se dice que dos conjuntos infinitos que tienen el mismo número cardinal son equivalentes. Sin embargo, un conjunto infinito puede ser equivalente a uno de sus propios subconjuntos. Por ejemplo, el conjunto de los enteros positivos n es equivalente al conjunto de los enteros positivos pares según se desprende de la correspondencia de n con $2n$. Debido a esta propiedad de los conjuntos infinitos, una correspondencia biunívoca entre los elementos del conjunto A y de un subconjunto propio de un conjunto B, significa solamente que el número cardinal del conjunto A es menor que o igual al número cardinal del conjunto B. Con el objeto de demostrar que el número cardinal de un conjunto A es menor que el número cardinal de un conjunto B, es necesario probar que A es equivalente a un subconjunto propio de B y que no existe una correspondencia biunívoca entre los elementos de A y los elementos de B.

Si un conjunto de elementos tiene un número cardinal tres, sus elementos pueden ordenarse en correspondencia biunívoca con el conjunto 1, 2, 3, de los enteros positivos. Si un conjunto está repre-

*Para la solución de este ejercicio se requiere la materia presentada en el Cap. I-11

sentado por un número cardinal n, sus elementos pueden ordenarse en correspondencia biunívoca con el conjunto 1, 2, 3 ... n, de enteros positivos. Si los elementos de un conjunto pueden ordenarse en correspondencia biunívoca con el conjunto de todos los enteros positivos 1, 2, 3, ..., su número cardinal se llama *Aleph-cero*, $\aleph_0$ y se dice que el conjunto es *infinito contable* o *infinito numerable*. El conjunto de todos los enteros positivos.

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \ldots \quad n \quad \ldots,$$

el conjunto de los enteros positivos pares

$$2 \quad 4 \quad 6 \quad 8 \quad 10 \quad 12 \quad 14 \ldots \quad 2n \quad \ldots,$$

el conjunto de los enteros positivos impares

$$1 \quad 3 \quad 5 \quad 7 \quad 9 \quad 11 \quad 13 \ldots \quad 2n-1 \ldots,$$

y aún el conjunto de los números racionales positivos, como lo demostraremos más adelante, son infinitos numerables.

El conjunto de los números racionales positivos es por lo menos infinito numerable, pues tiene como subconjunto al conjunto de los números enteros positivos. Demostraremos que el conjunto de los números racionales positivos es a lo sumo infinito numerable demostrando que el conjunto de todos los pares de enteros positivos es infinito numerable. Consideremos el cuadro

1/1	1/2	1/3	1/4	1/5	1/6	1/7	...
2/1	2/2	2/3	2/4	2/5	2/6	2/7	...
3/1	3/2	3/3	3/4	3/5	3/6	3/7	...
4/1	4/2	4/3	4/4	4/5	4/6	4/7	...
5/1	5/2	5/3	5/4	5/5	5/6	5/7	...
6/1	6/2	6/3	6/4	6/5	6/6	6/7	...
...	...	...	...	...	...	...	...

y asociemos un entero positivo con cada par siguiendo la dirección de las líneas diagonales tal como se indica en el cuadro:

$$1 \sim 1/1, \quad 2 \sim 1/2, \quad 3 \sim 2/1, \quad 4 \sim 3/1, \quad 5 \sim 2/2, \cdots$$

Esta correspondencia biunívoca entre el conjunto de los enteros positivos y el conjunto de todos los pares de enteros positivos indica que el conjunto de pares es infinito numerable. Dado que el conjunto de números racionales positivos es un subconjunto del conjunto de todos los pares de números enteros positivos, el conjunto de números racionales positivos no es superior a infinito numerable. Luego, ya que es también por lo menos infinito numerable, el conjunto de los números racionales positivos es infinito numerable.

La correspondencia anterior entre los números racionales positivos y los enteros positivos proporciona una ordenación de los números racionales positivos. Esta ordenación satisface las condiciones de un conjunto ordenado linealmente (Cap. 1 - 6), pero evidentemente no es una ordenación conforme a la magnitud o medida de los números. Por ejemplo, según este orden, 2 precede a $1/4$ y a 3.

Dado que el conjunto de los múltiplos de mil, el conjunto de los números enteros pares, el conjunto de los números enteros impares, el conjunto de los números enteros, y el conjunto de los números racionales tienen todos el mismo número cardinal, surge la cuestión de que si todos los conjuntos infinitos de números reales son infinitos numerables. Puede demostrarse que el conjunto de los números reales algebraicos es infinito numerable (Ejercicio 5) y que el conjunto de los números reales trascendentes no es infinito numerable (Ejercicio 6).

Si se representan únicamente los puntos enteros por medio de puntos sobre una recta, es fácil ver los "saltos" en la recta. Una vez que se han agregado todos los puntos racionales, los puntos se presentan densos y sin embargo, si se considera la recta como el eje de las x, y se describe el círculo con centro en el origen y radio $\sqrt{2}$, este círculo corta la recta sin encontrarse con ningún punto racional, de modo que debe haber aún "saltos" en la recta. Si se agregaran aún todos los puntos cuyas abscisas son números reales algebraicos (Cap. 1 - 10), todavía habría "saltos" ya que si la circunferencia de un círculo de radio igual a la unidad, pudiera cortarse, estirarse en línea recta colocando un extremo en el origen, el otro

extremo llegaría al punto trascendente 2π. Cuando se han representado todos los números reales no hay ningún "salto" en la recta.

Consideremos el conjunto de los números reales entre cero y uno y representémoslos como números decimales. Si el conjunto es infinito numerable, los decimales pueden ordenarse en correspondencia biunívoca con los enteros positivos y pueden escribirse en lista en el orden impuesto por esta correspondencia. Supongamos que el orden impuesto es

.1284 ...
.2315 ...
.1694 ...
.7850 ...
....
....

De acuerdo con la suposición de que el conjunto es infinito numerable, todos los decimales entre cero y uno se encuentran en el esquema anterior. Supongamos que formamos un decimal tomando los elementos .1390 ... de la diagonal principal y aumentamos cada elemento en 1, excepto el 9 que se reemplaza por 0. El nuevo decimal en este caso es .2401 ... y se encuentra entre el cero y el 1. Este decimal no se encuentra en la primera fila, ya que sus primeros elementos difieren; no está en la segunda fila, ya que sus segundos elementos difieren; y en general, no está en la j-ésima fila, puesto que los j-ésimos elementos difieren. De aquí que el decimal formado no se encuentre en el esquema, y que la suposición de que los números reales entre cero y uno son numerables nos ha conducido a una contradicción. En resumen, si el conjunto de los números reales entre cero y uno es infinito numerable, los números reales de ese conjunto pueden ponerse en una lista en algún orden como se hizo más arriba. Cualquiera que sea este orden, podríamos, si fuese necesario, volver a ordenar los números de modo que por lo menos uno de los dígitos de la diagonal principal no sea 8 sino 9 y, por medio de este procedimiento, formaríamos un nuevo decimal que no se encuentre en la lista. Por consiguiente, los números reales entre cero y uno no pueden ponerse en lista en ningún orden y el conjunto no es infinito numerable. Por esta razón el conjunto de los números reales es infinito, pero no infinito numerable, ya que uno de sus subconjuntos es infinito y no infinito numerable.

El número cardinal asociado con el conjunto de todos los números reales se llama el *número cardinal del continuo C.* El infinito numerable $\aleph_0$ es el primero, o sea el número cardinal transfinito menor. Uno de los problemas matemáticos famosos no resueltos es demostrar que C es el número transfinito siguiente a $\aleph_0$, es decir, $C = \aleph_1$. Hay por lo menos un conjunto infinito numerable de números cardinales transfinitos diferentes (ver Bibliografía Nº 13, págs. 84-85; y Nº 29, págs. 54-55), pero los dos anteriores son los más comunes.

La correspondencia entre los números reales y los puntos sobre una recta en la geometría euclidiana corriente, es válida sólo para números finitos. Los números transfinitos no se incluyen en el conjunto de los números reales y tienen relaciones completamente diferentes de las de los números reales. Por ejemplo, $\aleph_0 \pm a = \aleph_0$, donde a es igual a $\aleph_0$ o a cualquier número cardinal finito; $\aleph_0 + C = C$; $\aleph_0 \cdot 5 = \aleph_0$.

EJERCICIOS

1. Dar tres ejemplos de cada uno de los siguientes ejercicios: (a) un conjunto finito y un subconjunto finito propio; (b) un conjunto infinito y un subconjunto finito; (c) un conjunto infinito y un subconjunto infinito propio; (d) un conjunto infinito numerable; (e) un conjunto infinito que no sea infinito numerable.

2. Demostrar que los números racionales negativos son infinitos numerables.

3. Demostrar que cualquiera función $f(x)$ definida (Cap. III-10) para valores enteros positivos de x, toma una sucesión infinita numerable de valores (no necesariamente distintos) a medida que x toma los valores 1, 2, 3, ...

4. Dar tres ejemplos de sucesiones de números obtenidas como se señala en el Ejercicio 3.

5. Demostrar que el conjunto de los números reales algebraicos es infinito numerable (ver Bibliografía Nº 13; pág. 103).

6. Demostrar que el conjunto de números reales trascendentes no es infinito numerable

I-14 GRUPO; SISTEMA DE NUMEROS. Hemos estudiado el sistema de números racionales y el sistema de los números reales. En esta sección estudiaremos el concepto de

grupo y estableceremos con toda exactitud qué se entiende por un "sistema de números".

Un conjunto de elementos forma *un grupo* con respecto a una operación $\oplus$ binaria única cualquiera (Cap. I - 2) si ella es: (1) cerrada (2) asociativa; y contiene (3) un elemento de identidad; y (4) el inverso de cada uno de sus elementos. En otras palabras, el conjunto C de elementos $a, b, \ldots$ forma un grupo con respecto $a \oplus$ *si* (1) $a \oplus b$ está en C para todos los pares a, b de C; (2) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ para todo a, b, c, de C; (3) hay un elemento I de C tal que $I \oplus a = a \oplus I = a$ para todo elemento a de C; y (4) para todo a de C hay un elemento a' en C tal que $a \oplus a' = a' \oplus a = I$. Por ejemplo, el conjunto de los enteros (positivos, negativos y cero) forma un grupo con respecto a la operación de la adición pero no con respecto de la operación de la multiplicación. El conjunto de los números racionales (y también el conjunto de los números reales) forma un grupo con respecto a la adición. Si se excluye el cero, los números racionales restantes forman un grupo con respecto a la multiplicación.

Se dice que un grupo es *conmutativo* (o Abeliano) si $a \oplus b = b \oplus a$ para todos los elementos a, b, del grupo.

Un conjunto de elementos en el cual están definidas dos operaciones binarias $+$ y $\times$ forma un *sistema de números* o *campo conmutativo* si: (1) el conjunto forma un grupo conmutativo con respecto a $+$; (2) el conjunto, sin el elemento de identidad para $+$, forma un grupo con respecto a $\times$; y (3) las leyes de la distributividad de $\times$ con respecto a $+$,

$$a \times (b + c) = a \times b + a \times c, \quad (b + c) \times a = b \times a + c \times a,$$

son válidas para tres elementos cualesquiera a, b, c del conjunto. Un sistema de números en el cual la $\times$ es conmutativa se llama *campo**.

Si a y b son elementos de un sistema de números tal que $ab = 0$ y $a \neq 0$, entonces existe a^{-1} de acuerdo con (2), $a^{-1}ab = 0$, y $b = 0$. En otras palabras, si el producto de dos elementos de un sistema de números es cero, entonces por lo menos uno de los elementos debe ser cero. En rigor, un elemento $k \neq 0$ se llama un *divisor cero*

*Los autores franceses emplean el término "cuerpo". (N. de la T.).

si existe un elemento $j \neq 0$ tal que $j \cdot k = 0$ (ver Ejercicio 13, Cap. II - 9). La demostración anterior prueba que los divisores cero no pueden existir en un sistema de números.

Si un sistema de números contiene a los enteros positivos, debe contener también (i) a cero y a los enteros negativos, es decir, al elemento de identidad y a los inversos aditivos; y (ii) a los números racionales, ya que debe incluir a los inversos respecto a la multiplicación de todos los enteros diferentes de cero y a todas las sumas finitas de estos inversos. Por consiguiente, cualquier sistema de números que contiene a los enteros positivos debe contener a los números racionales. Los números racionales, los números reales, y —como veremos pronto— los números complejos, forman sistemas de números. Los conjuntos de los números racionales, reales y complejos forman también sendos campos, dado que hemos determinado que la adición y la multiplicación son operaciones conmutativas.

La definición exacta que hemos dado de un sistema de números contiene los conceptos básicos de este término matemático corriente. Es aún de mayor importancia fundamental la introducción de los conceptos de grupo y de campo que junto con el concepto de anillo (Cap. I - 18) forman la base de la mayoría de las definiciones del álgebra abstracta.

EJERCICIOS

1. Indicar cuáles de los conjuntos de números siguientes forman grupos respecto a la adición.

a) números enteros pares,

b) números enteros impares,

c) múltiplos enteros de diez,

d) múltiplos enteros de cualquier entero k,

e) enteros positivos,

f) números de la forma $b\sqrt{2}$ en que b es un número racional,

g) números de la forma $a + b\sqrt{2}$, en que a y b son enteros,

h) números de la forma $a + b\sqrt{2}$, en que a y b son números racionales,

i) 0,

j) números racionales positivos,

k) números irracionales,

l) números de la forma $a + bw$, donde a y b son números racionales cualesquiera y w es un número algebraico dado (Cap. I-18).

2. En cada uno de los conjuntos de números del Ejercicio 1, excluir el cero cada vez que se presente e indicar cuáles de los conjuntos de números que resultan forman grupos respecto a la multiplicación.

3. Demostrar que si en un conjunto de elementos la adición es asociativa, el conjunto es cerrado respecto a la sustracción y que este conjunto forma un grupo respecto a la adición.

1-15 LOS NUMEROS COMPLEJOS.

Hemos comenzado por los números enteros positivos, desarrollamos en seguida el sistema de números racionales con el fin de obtener un conjunto de números que sea cerrado para las cuatro operaciones racionales (adición, multiplicación, sustracción, división) e introdujimos el sistema de números reales para obtener un conjunto de números en el cual puedan representarse todas las magnitudes finitas. En los sistemas de números racionales y reales, las relaciones de orden e igualdad, así como las operaciones de adición y multiplicación tienen las mismas propiedades básicas que en el conjunto de los números enteros (Cap. 1-5 y Cap. 1-6). En esta sección repetiremos una vez más el procedimiento para definir las relaciones y operaciones para un nuevo símbolo, probando con respecto a un subconjunto de los símbolos, que estas definiciones son consistentes con las definiciones anteriores y definiendo los nuevos símbolos como números. Todos los símbolos finitos considerados anteriormente para los números podían ser representados como puntos sobre una recta en la geometría plana corriente y estaban linealmente ordenados. Los nuevos símbolos que consideraremos ahora deberán representarse sobre un plano en vez de sobre una recta en la geometría plana corriente. Por consiguiente, los nuevos símbolos no están ordenados linealmente y no consideraremos sus relaciones de orden.

Los nuevos símbolos que vamos a presentar son indispensables para resolver las ecuaciones algebraicas. Nuestro estudio anterior sobre los números algebraicos finitos puede considerarse desde otro punto de vista, a saber: encontrar números que correspondan a todas las raíces reales de una ecuación polinomia, es decir, números para designar los puntos en los cuales una curva polinómica corta el eje x en el plano real. Si a, b, c son enteros positivos arbitrarios, se necesitan los números racionales positivos para resolver todas las ecuaciones de la forma $ax = b$; a menudo se necesitan números

negativos para resolver ecuaciones de la forma $x + a = b$, y números reales (racionales y algunos irracionales) para resolver ecuaciones de la forma $ax^2 + bx + c = 0$ donde $b^2 - 4ac \geqq 0$. Todos los ceros de un polinomio $f(x)$ que *aparecen como intersecciones geométricas corrientes* del gráfico de $y = f(x)$ con el eje real x son, por supuesto, números reales. Sin embargo, algebraicamente conviene que la ecuación de segundo grado $x^2 + 2ax + b = 0$, tenga dos raíces, sea que la curva $y = x^2 + 2ax + b$ corte el eje x o no en la geometría plana de Euclides, es decir, para valores reales cualesquiera de a y b. En consecuencia, ampliaremos una vez más nuestro sistema de números para incluir un nuevo tipo de número.

Consideraremos ahora, pares ordenados de números reales (a, b) donde

(i) $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$;
(ii) $(a, b) + (c, d) = (a + c, b + d)$;
(iii) $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Como en el caso de otros símbolos nuevos, consideraremos una correspondencia entre un subconjunto $(a, 0)$ de los nuevos símbolos y el conjunto de los números reales a. También, como antes, las definiciones anteriores pueden usarse para demostrar que esta correspondencia es un isomorfismo (Ejercicio 1). Nótese que en este caso el isomorfismo no se denomina isomorfismo de orden.

Los nuevos símbolos (a, b) se definen como números, *números complejos,* para números reales cualesquiera a, b. El número a se llama la *parte real* del número complejo (a, b); b se llama la *parte imaginaria*. Se dice que el número complejo (a, b) es *imaginario* si $b \neq 0$, y que es *imaginario puro* si $b \neq 0$ y $a = 0$. Según el isomorfismo anterior el conjunto de los números complejos (a, b) comprende al conjunto de los números reales $(b = 0)$ y al conjunto de los números imaginarios $(b \neq 0)$. En vista de que los números complejos no están ordenados linealmente en cuanto a magnitud, la clasificación de números en positivos, cero y negativos se usa sólo para los números reales. De modo que los números negativos y positivos se refieren siempre a los números reales negativos y a los números reales positivos.

Ahora podremos demostrar que las raíces de $x^2 + 1 = 0$ son

$(0,1)$ y $(0, -1)$. Tenemos, en realidad $(0, 1)^2 = (0, 1) \cdot (0,1) = (0 - 1, 0 + 0) = (-1, 0) = -1$ y $(0, -1)^2 = (0, -1) \cdot (0, -1) = (0 - 1, 0 + 0) = (-1,0) = -1$. La manipulación mecánica de los números complejos se simplifica grandemente escribiendo $(0, 1) = i$. Entonces $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0,1 = a + bi$, y podemos considerar que a, b, i son números sujetos a la condición que $i^2 = -1$ todas las veces que aparezca i^2. Por consiguiente,

$$
\begin{aligned}
(2, 3)^3 = (2 + 3i)^3 &= 8 + 36i + 54i^2 + 27i^3 \\
&= 8 + 36i - 54 - 27i \\
&= -46 + 9i = (-46, 9).
\end{aligned}
$$

La palabra *complejo* denota que los nuevos números no son números simples, como se tenía entendido en el pasado, sino que cada uno es un par ordenado de números tales que satisfacen las condiciones (i) y (ii) anteriores. Es incorrecto emplear la palabra imaginario como opuesto a real. Excepto en el sentido técnico sobre el que están de acuerdo los matemáticos, las dos clases de números son igualmente reales.

Se puede considerar que los números negativos resultan de la rotación del eje positivo x en torno al origen en 180°. Si esta rotación se efectúa dos veces, se obtiene la identidad $-(-a) = a$. En este sentido, la multiplicación por -1 y la rotación en 180° son equivalentes (Fig. 1 - 2).

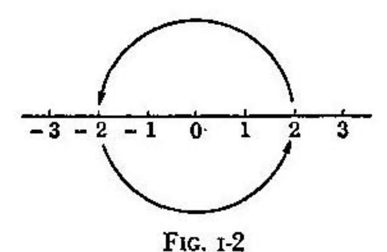


FIG. 1-2

De manera análoga, la multiplicación por i es equivalente a una rotación de 90°. Si la multiplicación o la rotación se aplica dos veces, se obtiene el número negativo y si se aplica cuatro veces, se obtiene el número original (Fig. 1 - 3).

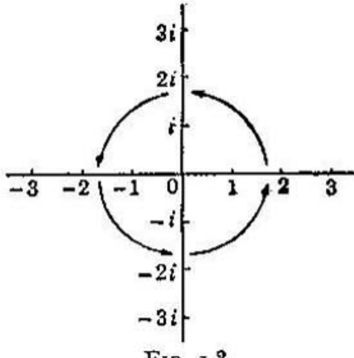


Fig. 1-3

Un plano tal como el de la Fig. 1 - 3 con un eje de números reales y un eje de los números imaginarios suele denominarse un *plano complejo.* Cada número complejo $a + bi = (a, b)$ puede asociarse con un punto único en el plano complejo con la coordenada a sobre el eje real y b sobre el eje imaginario (Cap. 1 - 16).

Los números complejos $a + bi$ y $a - bi$ son cada uno el *conjugado* del otro. La *norma* $n(z)$ de un número complejo z es el producto del número por su conjugado. Por eso si $z = a + bi$, $n(z) = n(a + bi) = (a + bi)(a - bi) = a^2 + b^2$, que para $z \neq 0$, es siempre positivo.

El *valor absoluto o módulo de* $z = a + bi$ es la raíz cuadrada no negativa de la norma $|z| = \sqrt{a^2 + b^2}$. De manera que el valor absoluto de un número complejo es siempre un número real.

Cuando buscamos el cuociente de dos números complejos $(a, b) \div (c, d)$, en realidad buscamos un número (p, q) tal que

$$(a, b) = (c, d) \cdot (p, q).$$

Tenemos

$$\begin{aligned}(a, b) &= (cp - dq, cq + dp),\\ a &= cp - dq,\\ b &= dp + cq,\end{aligned}$$

de donde

$$p = \frac{ac + bd}{c^2 + d^2}, \quad q = \frac{bc - ad}{c^2 + d^2}$$

si $c^2 + d^2 \neq 0$. Por consiguiente, de la unicidad de la suma, de la diferencia, del producto y del cuociente de los números reales, obte-

nemos números reales únicos p y q toda vez que $c^2 + d^2 \neq 0$, es decir, siempre que $(c, d) \neq 0$. Esto completa la demostración del teorema siguiente:

TEOREMA I - 1. *En el sistema de números complejos, la división es siempre posible y es única, con excepción de la división por cero.*

En la práctica, existe la costumbre de indicar la división de $z_1 = a + bi$ por $z_2 = c + di$ por medio del cuociente $z_1/z_2 = (a + bi) / (c + di)$. Este cuociente se expresa entonces como un número complejo multiplicando su numerador y su denominador por el conjugado de z_2, es decir,

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i.$$

En el Cap. I - 16 se estudian otras representaciones de z_1/z_2. En esa oportunidad trataremos también las relaciones entre los valores absolutos y los módulos de z_1 y z_2. En particular, necesitaremos demostrar que el valor absoluto de un producto de números complejos es igual al producto de los valores absolutos de sus factores. Este hecho es una consecuencia del Teorema I - 2, que formularemos y demostraremos en seguida.

TEOREMA I - 2. *La norma de un producto es igual al producto de las normas de sus factores.*

Sea $z_1 = a + bi, z_2 = c + di$, entonces $n(z_1) = a^2 + b^2, n(z_2) = c^2 + d^2, z_1z_2 = ac - bd + (ad + bc)i$, y además

$$\begin{aligned} n(z_1z_2) &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 + b^2d^2 - 2abcd + a^2d^2 + b^2c^2 + 2abcd \\ &= (a^2+b^2)(c^2+d^2) \\ &= n(z_1)\cdot n(z_2). \end{aligned}$$

Esto demuestra el teorema para el producto de dos factores. Dado que el producto de dos números complejos es también un número complejo, la demostración puede repetirse con $z_1 = w_1w_2, z_2 = w_3$

para demostrar el teorema para tres factores, y en general con $z_1 = w_1 w_2 \ldots w_{n-1}$ y $z_2 = w_n$ para demostrar el teorema para cualquier número finito de factores por inducción matemática (Cap. I - 4).

En el caso de la suma de los números complejos podemos demostrar

TEOREMA I - 3. *El valor absoluto de una suma de números complejos es menor que o igual a la suma de los valores absolutos.*

Supongamos $|z_1 + z_2| > |z_1| + |z_2|$ donde $z_1 = a + bi$, $z_2 = c + di$. Entonces

$$\sqrt{(a+c)^2 + (b+d)^2} > \sqrt{a^2+b^2} + \sqrt{c^2+d^2},$$

de donde

$$\begin{aligned}
(a+c)^2 + (b+d)^2 &> a^2 + b^2 + 2\sqrt{(a^2+b^2)(c^2+d^2)} + c^2 + d^2, \\
a^2 + c^2 + b^2 + d^2 + 2ac + 2bd &> a^2 + b^2 + c^2 + d^2 + 2\sqrt{(a^2+b^2)(c^2+d^2)}, \\
ac + bd &> \sqrt{(a^2+b^2)(c^2+d^2)}, \\
a^2c^2 + b^2d^2 + 2abcd &> a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2, \\
0 &> b^2c^2 - 2abcd + a^2d^2, \\
0 &> (bc - ad)^2.
\end{aligned}$$

Pero esto es imposible, dado que el miembro de la derecha es el cuadrado de un número real y por lo tanto no negativo. De esta manera la suposición de que el teorema es falso ha conducido a una contradicción, y hemos hecho una demostración indirecta (Cap. I - 10) del teorema para la suma de dos números complejos. Esta demostración puede ampliarse por inducción matemática y aplicarse a cualquier suma finita de la misma manera que se amplió la demostración anterior referente a los productos.

EJERCICIOS

1. Demostrar que la correspondencia de $(a, 0)$ respecto de a es un isomorfismo.

2. Valiéndose de conocimientos adquiridos previamente, proponer una ecuación de segundo grado con coeficientes reales que tenga sus raíces en el conjunto de (a) los números enteros, (b) los números racionales, (c) de los números reales irracionales, (d) de los números imaginarios, (e) los números imaginarios puros.

3. Demostrar que los números complejos forman un sistema de números.

4. Expresar en la forma $a + bi$:

$$\sqrt{-16},\quad 5,\quad -\tfrac{2}{3},\quad 1 + \sqrt{-2},\quad \frac{2 + \sqrt{-3}}{2 - \sqrt{-3}},\quad \frac{1}{3 + 4i}.$$

5. Determinar el módulo de cada uno de los números complejos dados en el Ejercicio 4.

6. Demostrar que si un número complejo es igual a su conjugado, el número es real.

7. Demostrar que si el producto de dos números complejos es cero, entonces por lo menos uno de los números es cero.

I - 16 PROPIEDADES DE LOS NUMEROS COMPLEJOS. Las relaciones entre el álgebra y la geometría son importantes especialmente para aquellas personas que intentan aprender los conceptos fundamentales de matemáticas. Hemos visto en el (Cap. I - 12) que todos los números reales pueden representarse como puntos sobre una recta e inversamente, todos los puntos de una recta en la geometría de Euclides pueden representarse por números reales. En esta sección del Cap. I consideraremos dos representaciones de números complejos en un plano euclidiano. En seguida, de estas representaciones gráficas deduciremos representaciones trigonométricas y exponenciales para los números complejos.

Dado un sistema ortogonal de coordenadas cartesianas de origen 0 y ejes $0x$ y $0y$, tomamos a $0x$ como el eje de los números reales y a $0y$ como el eje de los números imaginarios. El número complejo $z = a + bi$ puede representarse ya sea por el punto P: (a, b) o bien, si $z \neq 0$ por el segmento de recta orientado, *vector*, **OP** (Fig. I - 4).

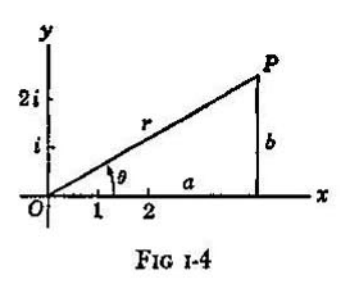


FIG I-4

Un vector tiene longitud y dirección. La longitud r de **OP** está dada por el valor absoluto de z; su dirección está dada por el ángulo θ formado por el eje positivo x y **OP**. Para cada z, el número no negativo $r = \sqrt{a^2 + b^2}$ está determinado unívocamente, pero $\theta =$ *arc tg* b/a, la *amplitud* o *argumento* de z, puede determinarse sólo dentro

de un múltiplo de 2π. El número complejo $z = a + bi$ y el punto $P:(a, b)$ están unívocamente determinados ya sea por el par de números reales (a, b), esto es, las coordenadas *ortogonales o cartesianas* del punto P, o por el par de números reales (r, θ), esto es, las *coordenadas polares* del punto P. Empleando funciones trigonométricas, $a = r\cos\theta$, $b = r\,\text{sen}\,\theta$, y $z = r$ $(\cos\theta + i\,\text{sen}\,\theta$. También puede expresarse cualquier número complejo z mediante notación exponencial.

Para números reales a, b el símbolo a^b puede definirse como un número real único (Ejercicio 13, Cap. I - 12) si $a = 0$ y $b > 0$; si $a > 0$ y b es cualquier número real; y cuando $a < 0$ y $b = r/s$ donde los enteros r, s no tienen factores comunes y s es impar. El valor único del símbolo a^b se basa en el hecho de que para los valores racionales de $b = r/s$, en que r, s son enteros sin factores comunes, la ecuación $x^s = a^r$ tiene una solución positiva única en el conjunto de los números reales cuando $a^r > 0$; y tiene una solución real única en todos los otros casos tales que a^b esté definido. Ya que la ecuación $x^s = a^r$ tiene s soluciones en el sistema de números complejos, el símbolo $a^{r/s}$ puede asociarse con cualquiera de los números complejos s. De aquí que, en nuestra definición de a^b en el sistema de números complejos, será necesario a veces designar un elemento particular de un subconjunto de los números complejos, como el *valor principal* de un símbolo dado a^b.

La representación exponencial $z = re^{i\theta}$, donde e es la base de los logaritmos naturales, puede deducirse de la representación trigonométrica $z = r(\cos\theta + i\,\text{sen}\,\theta)$ por medio de series infinitas. Los lectores que no recuerden las siguientes series infinitas de sus estudios anteriores de matemáticas, pueden revisar el desarrollo de estas series en el Cap. III - 15 o aceptar la representación $z = re^{i\theta}$ como una suposición más.

La serie infinita

$$e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

puede usarse para definir e^x para cualquier número complejo x (Cap. III - 15). Obtenemos entonces

$$e^{ix} = 1 + ix - \frac{x^2}{2} - \frac{ix^3}{3!} + \frac{x^4}{4!} + \frac{ix^5}{5!} - \cdots$$

substituyendo ix por x. Una comparación de esta serie con las dos series siguientes

$$\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots,$$

$$\operatorname{sen} x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$$

indica que $e^{ix} = \cos x + i \operatorname{sen} x$. De esta manera, tenemos tres representaciones para un número complejo, $z = a + bi = r$ $(\cos \theta + i \operatorname{sen} \theta = re^{i\theta}$. Las condiciones para la igualdad de dos números complejos z_1, z_2 son $a_1 = a_2$, $b_1 = b_2$, cuando los números están expresados en la primera forma. Cuando se emplean las otras dos formas las condiciones son $r_1 = r_2$, $\theta_1 = \theta_2 + 2k\pi$ para algún entero k. En general, encontraremos más útil la primera forma cuando estudiemos sumas de números complejos, y una de las otras formas cuando tratemos los productos o potencias.

La suma de $z_1 = a + bi$ y $z_2 = c + di$ se ha definido (Cap. 1-15) como $z_1 + z_2 = a + c + (b + d)i$. Para encontrar geométricamente la suma de dos números complejos z_1, z_2 representados por P_1 y P_2, respectivamente, se construye el paralelógramo que

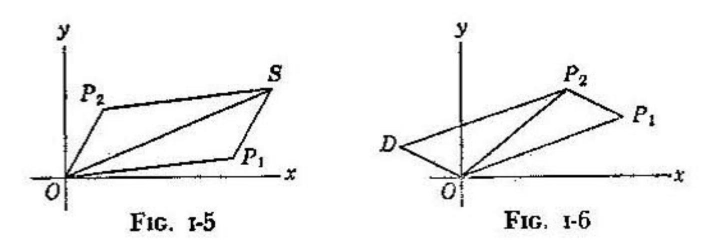


FIG. 1-5 FIG. 1-6

tiene OP_1 y OP_2 como lados (Fig. 1-5). La diagonal OS del paralelogramo es el vector que representa $z_1 + z_2$. La diferencia $z_2 - z_1$ puede construirse como un lado OD de un paralelogramo con diagonal OP_2 y un lado OP_1 (Fig. 1-6).

El producto z_1z_2 se define como $z_1z_2 = ac - bd + (ad + bc)i$, pero se interpreta con más facilidad en la forma $z_1z_2 = r_1e^{i\theta_1} \cdot r_2e^{i\theta_2} = r_1r_2e^{i(\theta_1 + \theta_2)}$. La fórmula $z_1z_2 = r_1r_2 [\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)]$ puede verificarse trigonométricamente. Luego, mediante la inducción matemática como en el Teorema 1-2, se tiene (Ejercicio 8).

TEOREMA I-4. *El valor absoluto del producto de dos o más números complejos es el producto de sus valores absolutos; el argumento del producto es la suma de sus argumentos.*

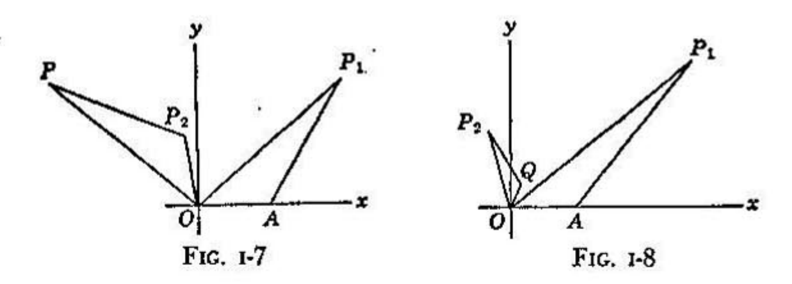


FIG. I-7 FIG. I-8

Para encontrar geométricamente el producto z_1z_2 representado por P_1P_2, constrúyase el triángulo OP_2P semejante al triángulo OAP_1 donde $O = (0,0)$ y $A = (1,0)$ (Fig. I-7). Entonces P es el punto que representa $z_1 \cdot z_2$. En esta construcción los dos triángulos OAP_1 y OP_2P deben estar orientados de manera análoga. Por ejemplo, si el interior del triángulo OAP_1 *está* a la izquierda al recorrer el perímetro del triángulo desde O hacia A, hacia P_1, hacia O, también el interior del triángulo OP_2P debe encontrarse a la izquierda al recorrer su perímetro en el sentido OP_2P. Los triángulos OAP_1 y OP_2P se encuentran orientados en forma análoga en la Fig. I-7; los triángulos OAP_1 y OP_2Q están orientados inversamente en la Fig. I-8.

La construcción geométrica correspondiente a un cuociente z_2/z_1 se obtiene construyendo los triángulos OP_2Q y OP_1A orientados en el mismo sentido (Fig. I-8). Por medio de $z_2/z_1 = (r_2/r_1)e^{i(\theta_2-\theta_1)}$ se obtiene el teorema correspondiente al Teorema I-4: el valor absoluto del cuociente de dos números complejos es el cuociente de sus valores absolutos; el argumento del cuociente es igual al argumento del dividendo menos el argumento del divisor.

Como en el caso de los números reales, las operaciones inversas de sustracción y división pueden evitarse calculando los números inversos $-z$ y $1/z$, respectivamente. Si $z = a + bi$, entonces $-z = -a - bi = r\,[\cos(\pi + \theta) + i \operatorname{sen}(\pi + \theta)] = re^{i(\pi+\theta)}$, de acuerdo con el Teorema I-4 y con $-1 = \cos\pi + i \operatorname{sen}\pi$. También si $r \neq 0$, $1/z = 1/r\,[\cos(-\theta) + i \operatorname{sen}(-\theta)] = 1/r\,(\cos\theta - i \operatorname{sen}\theta)$, aplicando el enunciado correspondiente para los cuocientes y también

$$1 = 1 \ (\cos 0 + i \operatorname{sen} 0).$$

Ya se ha examinado la suma, la diferencia, el producto y el cuociente de dos números complejos. Con la excepción de las relaciones de orden, todas las reglas anteriores se satisfacen en el sistema de números complejos. No hay ninguna definición satisfactoria de la magnitud o medida de un número complejo que pueda usarse para ordenar linealmente el conjunto de todos los números complejos. En efecto, hemos visto que los números complejos corresponden a los puntos de un plano en vez de a una línea recta. Por consiguiente, no cabría esperar que las relaciones de orden estudiadas anteriormente para los números reales se cumplieran para los números complejos. Los números complejos son densos y continuos, siempre que las definiciones de estos términos se formulen para conjuntos no lineales.

La importancia fundamental de los números complejos reside en el hecho de que ellos permiten calcular dos raíces para cualquiera ecuación de segundo grado $x^2 + 2ax + b = 0$, con coeficientes reales sin restricción respecto del signo de $a^2 - b$. En efecto, las n raíces de cualquier ecuación polinomia de grado n (Cap. III-1 y Teorema IV-2) con coeficientes complejos pueden expresarse como números complejos (Cap. I-18). Esta propiedad se explica diciendo que el sistema de los números complejos es *cerrado algebraicamente* (ver Bibliografía Nº 7, pág. 393). Las raíces de las ecuaciones $w^2 = z$, $w = z^2$ y, en general, $w^n = z$, $w = z^n$ para cualquier entero positivo n y para cualquier número complejo dado z han sido de particular interés para los matemáticos y se estudiarán en el Cap. I-17.

EJERCICIOS

1. Expresar cada uno de los siguientes números complejos en la forma $r(\cos\theta + i \operatorname{sen}\theta)$:

a) $1 + i$, c) 15, e) $-8 + 8i\sqrt{3}$,

b) $2 - 2i$, d) $7i$, f) -3.

2. Expresar cada uno de los números complejos del Ejercicio 1 en la forma $re^{i\theta}$.

3. Sumar gráficamente los siguientes pares de números:

(a) $3 - i$, $5 + 2i$, (c) $\sqrt{5} - \sqrt{-1}$, $2 - \sqrt{-16}$,

(b) $3 + \sqrt{-27}$, i, (d) $2 + 2\sqrt{-3}$, $\dfrac{1 + i\sqrt{2}}{2}$.

4. Multiplicar gráficamente los pares de números del Ejercicio 3 y comprobar las respuestas algebraicamente.

5. Sustraer gráficamente el primer número del segundo en cada ítem del Ejercicio 3 y comprobar las respuestas algebraicamente.

6. Dividir gráficamente el primer número por el segundo en cada ítem del Ejercicio 3 y comprobar las respuestas algebraicamente.

7. Establecer las condiciones necesarias para que sean válidas las siguientes igualdades:

$$\text{(a)}\ |z_1 + z_2| = |z_1| + |z_2|,$$
$$\text{(b)}\ |z_1 - z_2| = |z_1| - |z_2|.$$

8. Demostrar el Teorema 1-4.

1-17 TEOREMA DE DE MOIVRE.

Dado cualquier número complejo $z = re^{i\theta}$ y cualquier entero positivo n, se ha establecido que z^n representa el producto de n factores z. Luego, de acuerdo con el Teorema 1-4, se tiene $z^n = r^n e^{in\theta}$. De manera análoga, para cualquier número complejo dado $z = re^{i\theta}$ y cualquier entero positivo n, las n raíces complejas de la ecuación $w^n = z$ pueden expresarse en la forma:

$$z^{1/n} = (re^{i\theta})^{1/n} = r^{1/n}e^{(\theta+2k\pi)i/n}$$

para $k = 0, 1, 2, ..., n - 1$, teniendo en cuenta que θ está determinado sólo para valores dentro de los límites de un múltiplo de 2π. Los valores $k = n, n+1, ...$, no se usan, dado que el seno y el coseno $(\theta + 2k\pi)/n$ tienen valores iguales para $k = n$ y $k = 0$, para $k = n+1$ y $k = 1$, ... Sin embargo, en ambos casos z^n y $z^{1/n}$, los resultados se obtienen y se recuerdan más fácilmente por medio de las reglas corrientes para los exponentes.

El símbolo z^n tiene un valor único para cualquier entero positivo n. El símbolo $z^{1/n}$ puede tomar cualquiera de los valores de n en el sistema de números complejos. Si z es un número real, los valores posibles del símbolo $z^{1/n}$ incluyen el valor real representado por $z^{1/n}$ en el conjunto de los números reales. Este valor se llama el valor principal (Cap. 1-16) de $z^{1/n}$ en el conjunto de los números complejos. Puede obtenerse haciendo $k = 0$ cuando z es positivo, y haciendo $k = (n - 1)/2$ cuando z es negativo y n es impar. Cuando z es negativo y n es par, el valor principal de $z^{1/n}$ se obtiene ha-

ciendo $k = 0$. No intentaremos designar valores principales para $z^{1/n}$ cuando z es imaginativo.

Consideremos, por ejemplo, $z = 2 + 2i\sqrt{3}$ con $r = 4$ y $\theta = 60^\circ = \pi/3$, es decir, $z = 4e^{\pi i/3}$. Tenemos entonces $z^2 = 16e^{2\pi i/3}$ y $z^{1/2} = 2e^{(\pi/3+2k\pi)i/2}$, donde $k = 0,1$. Usaremos, en seguida, la relación $e^{ix} = \cos x + i \operatorname{sen} x$ (Cap. 1-16) para expresar z^2 y $z^{1/2}$ en la forma $a + bi$. En particular, $z^2 = 16 (\cos 2\pi/3 + i \operatorname{sen} 2\pi/3) = 16 (\cos 120^\circ + i \operatorname{sen} 120^\circ) = -8 + 8i\sqrt{3}$. Para $k = 0$, $z^{1/2} = 2 (\cos \pi/6 + i \operatorname{sen} \pi/6) = \sqrt{3} + i$; para $k = 1$, $z^{1/2} = 2 (\cos 7\pi/6 + i \operatorname{sen} 7\pi/6) = -\sqrt{3} - i$. Si hacemos $k = 2$, entonces $z^{1/2} = 2 (\cos 13\pi/6 + i \operatorname{sen} 13\pi/6) = 2 (\cos \pi/6 + i \operatorname{sen} \pi/6)$, y obtendremos el mismo valor de $z^{1/2}$ que para $k = 0$. El teorema siguiente enuncia en forma general estos resultados.

TEOREMA 1-5. TEOREMA DE DE MOIVRE. *Si n es un entero positivo cualquiera y $z = r (\cos \theta + i \operatorname{sen} \theta)$, entonces,*

$$z^n = [r(\cos \theta + i \operatorname{sen} \theta)]^n = r^n(\cos n\theta + i \operatorname{sen} n\theta) = r^n e^{in\theta};$$

$$z^{1/n} = r^{1/n}\{\cos [(\theta + 2k\pi)/n] + i \operatorname{sen} [(\theta + 2k\pi)/n]\}.$$

$$= r^{1/n}e^{i(\theta+2k\pi)/n}, \quad k = 0, 1, 2, \ldots, n - 1.$$

Este teorema se aplica a cualquier número complejo $z = re^{i\theta}$ y a enteros positivos n para expresar el número complejo único z^n y las n raíces complejas de la ecuación $w^n = z$. Cada una de estas n raíces tiene el valor absoluto $r^{1/n}$, es decir, cada una está representada por un punto en un círculo de radio $r^{1/n}$ con centro en el origen. Estos puntos están situados a iguales distancias sobre el círculo, ya que, cuando se calculan en el orden de los valores correspondientes de k, sus amplitudes difieren en múltiplos consecutivos de $2\pi/n$. En el ejemplo anterior de $z = 2 + 2i\sqrt{3}$, las dos raíces de $w^2 = z$ tenían amplitudes de $\pi/6$ y $\pi/6 + 2\pi/2 = 7\pi/6$, respectivamente, y ambas tenían el valor absoluto 2. En general se tiene,

TEOREMA 1-6. *Cualquier número complejo $z = r (\cos \theta + i \operatorname{sen} \theta)$ no igual a cero tiene exactamente n raíces complejas distintas de orden n que pueden representarse por n puntos situados a distancias iguales sobre un círculo de radio $r^{1/n}$.*

En particular, para $z = 1$, las raíces cúbicas de la unidad satisfacen,

$$w^3 = 1 = 1 \ (\cos 0 + i \text{ sen } 0)$$

y, por lo tanto, puede expresarse como,

$$w = 1^{1/3} \left[\cos (0 + 2k\pi)/3 + i \text{ sen } (0 + 2k\pi)/3\right]$$

para $k = 0, 1, 2$ o como,

$$w_1 = 1 \ (\cos 0 + i \text{ sen } 0) = 1,$$
$$w_2 = 1 \ (\cos 120^\circ + i \text{ sen } 120^\circ) = -\tfrac{1}{2} + i\sqrt{3}/2,$$
$$w_3 = 1 \ (\cos 240^\circ + i \text{ sen } 240^\circ) = -\tfrac{1}{2} - i\sqrt{3}/2.$$

Los puntos que representan w_1, w_2, w_3, son los vértices de un triángulo equilátero inscrito en un círculo de radio igual a la unidad con el origen por centro y que tiene un vértice en (1,0) sobre el eje positivo x. En general, las n-ésimas raíces de la unidad están representadas por los vértices de un polígono regular de n lados inscrito en el círculo de radio unidad, con un vértice en (1,0) sobre el eje positivo x.

Considerado desde un punto de vista ligeramente diferente, las n-ésimas raíces de la unidad forman un grupo (Cap. I - 14) de n elementos. Se llama un *grupo cíclico,* ya que todo elemento del grupo puede expresarse en función de un solo elemento. En el ejemplo anterior, $w^3 = 1$, las tres raíces pudieron expresarse como w_2, w_2^2, w^3_2, o como w_3, w^2_3, w^3_3. Una raíz n-ésima de la unidad, es una *raíz n-ésima primitiva* de la unidad si n es el entero positivo menor m tal que $s^m = 1$, es decir, según la terminología de la teoría de grupos, las raíces n-ésimas primitivas son aquéllas de *orden n*.

Según el Teorema de De Moivre, las raíces n-ésimas de la unidad que se obtienen de $z^n = \cos 0 + i \text{ sen } 0 = 1$ son $\cos 2k\pi/n + i$ sen $2k\pi/n$ siendo $k = 0, 1, 2, \ldots, n - 1$. En particular, para $k = 1$ la raíz $w = \cos 2\pi/n + i \text{ sen } 2\pi/n$ es una raíz n-ésima primitiva, dado que $w^t = \cos 2t\pi/n + i \text{ sen } 2t\pi/n$ puede igualarse a la unidad si y sólo si t es un múltiplo de n, es decir, si n es la potencia positiva menor de w que es igual a la unidad. Por consiguiente, existe por lo menos una raíz n-ésima primitiva de la unidad para cualquier entero positivo n. Procederemos ahora a encontrar todas las raíces n-ésimas (no necesariamente primitivas) a partir de una sola raíz n-ésima primitiva de la unidad.

Dada cualquiera raíz n-ésima primitiva de la unidad s y cualquier entero t, se tiene $(s^t)^n = (s^n)^t = 1^t = 1$, de donde cualquier potencia entera positiva de una raíz n-ésima primitiva es también

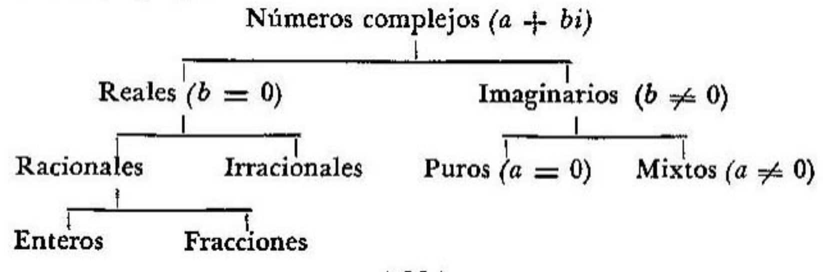
una raíz n-ésima de la unidad. También, si $s^t = s^u$, podemos suponer que $u \leqq t$ y escribir $s^{t-u} = 1$. Pero n es la potencia menor de s que es igual a la unidad, puesto que s es una raíz n-ésima primitiva. De aquí que, o bien $t = u$ o $t - u$ es un múltiplo de n (Cap. II - 2 y Teorema II - 8), es decir, $s^t = s^u$ si y sólo si $t = u + kn$ para algún entero k. En consecuencia, hemos demostrado que los números $s, s^2, s^3, \ldots, s^n = 1$ son raíces n-ésimas distintas de la unidad. Conforme a la suposición (Teorema IV - 2) de que la ecuación polinomia $z^n - 1 = 0$ tiene n raíces, se tiene el

TEOREMA I-7. *Si es es una raíz n-ésima primitiva de la unidad, todas las raíces n-ésimas de la unidad están dadas por la sucesión*

$$s, s^2, s^3, \ldots, s^{n-1}, s^n = 1.$$

Más adelante encontraremos (Teorema II - 17) que las raíces n-ésimas primitivas de la unidad son precisamente los números s^t en donde t y n son primos entre sí y s es cualquiera raíz n-ésima primitiva de la unidad.

El estudio de los grupos es de considerable importancia en las teorías matemáticas. Los examinaremos más adelante a medida que estudiemos unos cuantos conceptos abstractos más en el Cap. I - 18. Hasta aquí hemos considerado las propiedades de los enteros positivos (Cap. I-4) y a partir de éstos hemos desarrollado los sistemas de los números racionales, reales y complejos y hemos examinado las aplicaciones y las ventajas de cada sistema. Aceptando algunas igualdades tales como $a + 0 \cdot i = a$ y $a/1 = a$, podemos considerar que el sistema de números complejos es "nuestro sistema de números" y que los otros conjuntos de números son subconjuntos de él. El cuadro siguiente señala algunas de estas subdivisiones del sistema de números complejos y las condiciones que se establecen en cada caso para los números reales a, b, en la expresión $a + bi$ del número complejo general.



Los números reales pueden también clasificarse en positivos, cero o negativos; y los números complejos en algebraicos o trascendentes.

El sistema de números complejos puede considerarse de este modo como la base de nuestro estudio sobre los conceptos fundamentales del álgebra. El próximo capítulo, la teoría elemental de los números, se ocupa de algunas propiedades especiales de los números enteros. En particular, se considerarán propiedades suficientes para demostrar que todos los decimales periódicos representan números racionales y a la inversa (Cap. II - 7). Los polinomios tienen muchas propiedades análogas a aquéllas de los enteros y en el Capítulo III se hace un estudio paralelo de la teoría de los polinomios antes de tratar la teoría de las ecuaciones polinomias en el Capítulo IV.

EJERCICIOS

1. Sin emplear el Teorema de De Moivre, encontrar las raíces cuadradas de $11 - 60i$, $5 + 12i$, $-i$, $24 + 70i$, $-4ab + (2b^2 - 2a^2)i$.

(Indicación: suponer que $\sqrt{z} = x + iy$, y determinar x e y).

2. Encontrar z mediante el Teorema de De Moivre en los siguientes casos: $z^4 = 16$; $z^3 = -27$; $z^4 = i$; $z^3 = 8i$, $2^3 = 4 + 4\sqrt{-3}$.

3. Desarrollar $(\cos\theta + i \operatorname{sen}\theta)^3$ mediante el Teorema de De Moivre. Desarrollarlo también por medio del teorema del binomio y obtener de este modo fórmulas para $\cos 3\theta$ y $\operatorname{sen} 3\theta$.

4. Demostrar que los números $1, -1, i, -i$ forman un grupo (Cap. I-14) respecto de la multiplicación.

5. Encontrar las cinco raíces de la unidad y representarlas gráficamente.

6. Encontrar todos los valores de $\sqrt[5]{1 + i}$ y de $\sqrt[3]{i}$ y representarlos gráficamente.

7. Desarrollar valiéndose del Teorema de De Moivre:

$(2\sqrt{3} - 2i)^5$; $[4(\cos 150° + i \operatorname{sen} 150°)]^4$

8. Encontrar las tres raíces cúbicas de -27, $-i$, $1 + i$.

9. Si w, w' son las raíces cúbicas complejas conjugadas de la unidad, demostrar que

$1 + w + w^2 = 0$, $w' = w^2$, $w = w'^2$, $w \cdot w' = 1$.

10. Indicar las raíces de la ecuación $z^n - 1 = 0$.

11. Hacer un cuadro señalando cuáles de los catorce conjuntos de números (complejos, imaginarios, imaginarios puros, imaginarios mixtos, reales, racionales, irracionales, enteros, fraccionarios, positivos, cero, negativos, algebraicos, trascen-

dentes) mencionados anteriormente son cerrados (Cap. 1-2) respecto a (a) la adición; (b) a la sustracción; (c) la multiplicación; (d) la división.

12. Hacer un cuadro como en el Ejercicio 11, señalando cuáles de los catorce conjuntos de números son (a) grupos respecto a la adición; (b) grupos respecto a la multiplicación, después de excluir el cero de aquellos conjuntos que contienen el cero; (c) campos (es decir, sistemas de números conmutativos).

13. Demostrar que las raíces n-ésimas de la unidad forman un grupo cíclico para cualquier entero positivo n.

1-18* CAMPOS Y SISTEMAS DE NUMEROS. La analogía a que nos referimos anteriormente entre las propiedades de los polinomios y las de los números enteros se debe a que ambos conjuntos forman anillos (se definirán en breve). En la presente sección estudiaremos unos cuantos conceptos fundamentales pero algo abstractos relacionados con nuestro sistema de números. Los conceptos de grupo, campo y sistema de números se han definido en el Cap. 1-14. En esa sección (Cap. 1-14) se mostró también que el conjunto de los números racionales forma el campo menor (sistema de números conmutativos) que contiene a los enteros positivos. En la presente sección consideraremos un estudio de los números complejos por adjunción (se definirá luego) de números a los conjuntos de los números racionales y reales. Observaremos también que el conjunto de los números complejos forma un campo en el cual toda ecuación polinomia de una incógnita con coeficientes pertenecientes al sistema de números complejos puede factorizarse en factores lineales.

Empezaremos con los enteros positivos o números naturales. Con el objeto de formar un grupo respecto de la adición debemos incluir los enteros negativos y cero. El conjunto de todos los enteros forma un anillo. En general, un conjunto de elementos para los cuales la adición y la multiplicación están definidas unívocamente, forma un *anillo* si los elementos del conjunto

(i) forman un grupo conmutativo respecto de la adición;
(ii) son cerrados con respecto a la multiplicación;
(iii) satisfacen la ley asociativa de la multiplicación, y
(iv) satisfacen la ley distributiva de la multiplicación con respecto a la adición (Cap. 1-14).

El conjunto de los números enteros pares satisface la definición anterior y forma un anillo. Por consiguiente, existen anillos de

números que no contienen a la unidad, el elemento de identidad para la multiplicación.

Un *campo* puede definirse como un anillo en el cual

(*i*) hay un elemento de identidad, la unidad, con respecto a la multiplicación;

(ii) la multiplicación es conmutativa, y

(iii) todos sus elementos, con excepción de cero, tienen un inverso respecto de la multiplicación.

Por consiguiente, cualquier conjunto de elementos (por ejemplo, el conjunto de los números racionales, reales o complejos) que forma un campo, forma también un anillo, pero no a la inversa. Los números enteros forman un anillo, pero no forman un campo. En general, los elementos de un anillo o de un campo no son necesariamente números. Por ejemplo, el conjunto de todos los polinomios en la variable x con coeficientes enteros forma un anillo; el conjunto de todas las funciones racionales en x con coeficientes enteros forma un campo. Un amplio tratado de grupos, anillos, y campos se puede consultar en las Bibliografías N.os 7 y 52 y un estudio muy ameno en el Nº 34 de la misma.

En el Cap. 1 - 8 ampliamos el conjunto de los enteros positivos considerando cuocientes a/b donde a y b eran enteros positivos. En general, podemos asociar con cualquier anillo los cuocientes a/b donde a y $b \neq 0$ sean elementos de un anillo y b no sea un divisor cero (Cap. 1 - 14). Este conjunto de cuocientes forma un campo y se denomina el *campo cuociente* del anillo. Por consiguiente, el campo cuociente del anillo de los enteros es el campo de los números racionales, R.

El campo R puede ampliarse por *adjunción* (tal como se describe en la frase que sigue) de un elemento k que no pertenezca a R. El campo ampliado se compone de todos los cuocientes (denominador diferente de cero) de los polinomios en k con coeficientes pertenecientes a R. Si k es un elemento de R no se obtiene nada nuevo. El conjunto de todos los polinomios en k con coeficientes pertenecientes a R forma un anillo que se designa por $R[k]$. El conjunto de todas las funciones racionales de k (cuocientes de polinomios en que el polinomio del denominador es diferente de 0) con coeficientes pertenecientes a R forma un campo que se designa por $R(k)$.

El campo $R(k)$ se llama una *ampliación algebraica* del campo R si k es una raíz de un polinomio $f(x)$, no idéntico a cero, con coeficientes pertenecientes a R.

Por ejemplo, el anillo $R[\sqrt{2}]$ comprende a todos los números de la forma $a + b\sqrt{2}$, donde a y b pertenecen a R; el campo $R(\sqrt{2})$ también comprende a todos los números $a + b\sqrt{2}$, ya que

$$\frac{c + d\sqrt{2}}{e + h\sqrt{2}} = \frac{c + d\sqrt{2}}{e + h\sqrt{2}} \cdot \frac{e - h\sqrt{2}}{e - h\sqrt{2}} = a + b\sqrt{2}$$

para un valor adecuado de a y b en R. En general, el anillo $T[k]$, que se obtiene por adjunción de un número k que es algebraico con respecto a T, en un campo T, es también un campo, es decir, $T[k] = T(k)$ cuando k es algebraico con respecto a T. Empleando una terminología que no se ha definido en este capítulo pero que es familiar a casi todo el mundo, podemos demostrar el enunciado anterior de la manera siguiente: supongamos que $f(k) = 0$ y consideremos $g(k)/h(k)$ en donde $f(x)$, $g(x)$ y $h(x)$ son polinomios, $f(x)$ es irreducible con respecto a T, y $h(k) \neq 0$. Luego, $f(x)$ y $h(x)$ tienen como máximo factor común a la unidad, de donde, según el Algoritmo de Euclides (Cap. III - 7) resultan polinomios $p(x)$ y $q(x)$ tales que

$$p(x)f(x) + q(x)h(x) = 1.$$

Dado que $f(k) = 0$, tenemos $q(k)h(k) = 1$, de donde

$$\frac{g(k)}{h(k)} = g(k) \cdot q(k)$$

es un polinomio en k, es decir, $T[k] = T(k)$.

Finalmente, dado el anillo de los enteros con campo cuociente R, buscamos un campo T tal que todo polinomio $f(x)$ con coeficientes pertenecientes a R, se factorice completamente en factores lineales (cada uno con coeficientes pertenecientes a T). Dado que $f(x)$ puede ser lineal, todo elemento de R es un elemento de T. Por consiguiente, T es un campo ampliado de R. Supongamos que tratáramos de construir T por adjunción de números a R. Con el objeto de factorizar $x^2 - 2$ se debe adjuntar $\sqrt{2}$ y se obtiene $R(\sqrt{2})$. Análogamente, para cualquier número primo 2, 3, 5, 7, 11, 13, 17, ... se debe adjuntar $\sqrt{p}$ con el objeto de factorizar

$x^2 - p$ en factores lineales. En el Cap. II - 3 se demostrará que existen infinitos números primos. Por consiguiente, no bastará ningún número finito de adjunciones a R de la forma $\sqrt{p}$, ni aun para factorizar todas las expresiones cuadráticas de la forma $x^2 - p$, y por lo tanto, es necesario enfocar el problema de algún otro modo.

Una manera de abordar este problema implica el concepto de continuidad (Cap. I - 12), y por lo tanto se necesita para esto el campo R^* de los números reales. El campo R^* contine $\sqrt{p}$ de todos los números primos p y por consiguiente es suficiente para factorizar polinomios de la forma $x^2 - p$. Ya que los números reales son infinitos no se puede esperar obtener R^* por medio de un número finito de ampliaciones algebraicas de R.

El campo de los números complejos R^* (i) constituye una ampliación algebraica de R^*, dado que i satisface la ecuación $x^2 + 1 = 0$. Se puede demostrar también que el campo R^* *(i)* no puede ampliarse más, algebraicamente, es decir, que todo polinomio de grado positivo con coeficientes pertenecientes a R^* *(i)* tiene todas sus raíces en R^* *(i)*. Este resultado se demuestra frecuentemente en dos etapas. Primero se demuestra el Teorema Fundamental del Algebra (Teorema IV - 3) : Todo polinomio $p(x)$ de grado positivo con coeficientes complejos tiene por lo menos un cero complejo. En seguida se demuestra el Teorema IV - 2: Todo polinomio de grado $m > 0$ con coeficientes complejos tiene precisamente m ceros complejos (no necesariamente distintos). Existen varias demostraciones del Teorema Fundamental del Algebra, y todas implican conceptos no algebraicos (ver Bibliografía Nº 7; pág. 114). Por este motivo, se remite al lector a la (Bibliografía Nº 7; págs. 113-115) y a otros textos análogos en busca de una prueba intuitiva. En el Capítulo IV adoptaremos el Teorema IV - 3 sin demostración y lo aplicaremos en la demostración del Teorema IV - 2. Se puede demostrar también (Bibliografía Nº 7; pág. 393) que todo polinomio con coeficientes algebraicos tiene todas sus raíces en el conjunto de los números algebraicos (Cap. I - 10). En otras palabras, cualquier polinomio con coeficientes algebraicos puede factorizarse en factores lineales con coeficientes algebraicos. En la mayoría de los textos de álgebra abstracta puede consultarse una explicación más amplia de los temas tratados en esta sección.

EJERCICIOS

1. Demostrar que el conjunto de los números de la forma $3n$, donde n es un entero, forma un anillo.

2. ¿Forman los decimales exactos (Cap. I-10) un grupo respecto de la adición? ¿Un anillo?

3. Determinar cuáles de los conjuntos de números del Ejercicio 1, Cap. I-14, forman anillos.

4. ¿Cuáles de los catorce conjuntos de números del Ejercicio 11, Cap. I-17, forman anillos?

5. Demostrar que $R[\sqrt{3}] = R(\sqrt{3})$.

6. Demostrar en forma intuitiva y por escrito que los números complejos son cerrados algebraicamente.

7. Demostrar que $R[\sqrt[3]{2}] = R(\sqrt[3]{2})$.

8. Demostrar que $R[\sqrt[4]{2}] = R(\sqrt[4]{2})$.

CAPITULO II

Teoría de los números

Las propiedades de los enteros —positivos, negativos y cero— pueden aprovecharse para resolver varios tipos de problemas. Ellas son también de una importancia considerable en las teorías matemáticas. Por esta razón continuaremos nuestro estudio del sistema de números y examinaremos algunas de las propiedades especiales del conjunto de los números enteros. Según las definiciones y postulados enunciados en el Capítulo I, los enteros

(i) forman un grupo conmutativo con respecto a la adición (Cap. I - 14);

(ii) son cerrados con respecto a la multiplicación (Cap. I - 5);

(iii) satisfacen la ley asociativa de la multiplicación (Cap. I - 5), y

(iv) satisfacen la ley distributiva de la multiplicación con respecto a la adición (Cap. I - 5).

Estas cuatro propiedades son precisamente las condiciones necesarias para que un conjunto de elementos forme un anillo (Cap. I - 18). En consecuencia, nos referiremos al conjunto de los números enteros con el nombre de *anillo de los enteros.*

El anillo de los números enteros tiene también otras tres propiedades (Cap. I - 5 y Cap. I - 14) que no son necesarias para todos los anillos:

(i) la multiplicación es conmutativa;
(ii) hay un elemento de identidad respecto de la multiplicación, que es la unidad en el anillo, y
(iii) no hay en el anillo divisores cero.

Técnicamente, estas últimas propiedades determinan que el anillo de los números enteros constituya también un *dominio de integridad.*

En este capítulo nos preocuparemos principalmente de las propiedades del anillo de los enteros. Muchas de estas propiedades son también propiedades de anillos más generales y se estudiarán como propiedades del anillo de los polinomios en el Capítulo III.

II · 1 DIVISIBILIDAD. En un campo tal como el sistema de los números racionales o el sistema de los números reales, todo elemento del campo distinto de cero es divisor de cualquier otro elemento. En un anillo, tal como el anillo de los números enteros, no se puede suponer la divisibilidad de un elemento a por un elemento $b \neq 0$. Por definición, un entero b es divisor *o factor* de un entero a (se escribe $b|a$) si y sólo si $a = bc$, en donde c es un entero. Por ejemplo, $2|6$, $3|12$ y 3 es divisor de 15, pero 3 no es divisor de 8. El hecho de que si $c = 0$ todo entero $b \neq 0$ es divisor de cero, no debe confundirse con el concepto de "divisor cero" (Cap. I - 14) que se usa sólo cuando b y c son diferentes de cero. Aplicando la definición anterior, tenemos el teorema siguiente respecto de los enteros a, b, c.

TEOREMA II - 1. *Si c es divisor de b y b es divisor de a, entonces c es divisor de a. Si c es divisor de a y c es divisor de b, entonces c es divisor de $a + b$ y también de $a - b$.*

Un ejemplo de la primera parte del teorema sería $4|12$, $12|36$, y por lo tanto $4|36$. Asimismo, un ejemplo para la segunda parte del teorema sería $4|12$ y $4|32$ y por lo tanto $4|44$ en que $44 = 32 + 12$, y también $4|20$ en que $20 = 32 - 12$. Estas propiedades pueden demostrarse para enteros arbitrarios a, b, c que satisfagan las condiciones del teorema.

En la primera parte del teorema se da la condición de que c sea divisor de b y de que b sea divisor de a; es decir, existen enteros r y s tales que $b = cr$ y $a = bs$. Luego, puesto que la multiplicación es asociativa, $a = (cr)s = c(rs)$, de donde c es factor de a. Según la última parte del teorema existen enteros p y q tales que $a = cp$ y $b = cq$ de donde, según la ley distributiva de la multiplicación con respecto a la adición, $a + b = c(p + q)$ y $a - b = c(p - q)$. Esto completa la demostración del teorema.

Un número e se llama *unidad* si e es divisor de todos los elementos del conjunto. Las unidades en el anillo de los números enteros son $+1$ y -1. Sin embargo, solamente $+1$ es la unidad, o sea, el elemento de identidad respecto de la multiplicación.

El número entero 2 es un divisor común de 12 y 30. Los enteros -2, 3, -3, 6 y -6 son también divisores comunes de 12 y 30. Sin embargo, 6 es el único divisor común positivo de 12 y 30 que es divisible por todos los otros divisores comunes. Por eso se llama a 6 el máximo común divisor de 12 y 30. En general, enunciaremos las siguientes definiciones: Si c es divisor de a y c es divisor de b, entonces c es un *divisor común* de a y de b. Si c es un divisor común positivo de a y b, y todo otro divisor común d de a y b es divisor de c, entonces c es el *máximo común divisor* (MCD) de a y b, y se escribe $c = (a, b)$. Un entero cualquiera ec en donde $c = (a, b)$ y e es una unidad suele llamarse un MCD de a y b. Hemos modificado la definición corriente y determinado explícitamente al MCD positivo como *el* MCD de modo que el MCD esté unívocamente definido y coincida con el significado que se acepta para el símbolo (a, b). Luego, para cualquier conjunto finito de enteros a_1, a_2, $\ldots$, a_n, que no sean todos cero, podemos definir un máximo común divisor positivo único $c = (a_1, a_2, \ldots, a_n)$ que tenga la propiedad que todos los divisores comunes del conjunto, sean divisores de c. Tómese nota que c es divisor de c puesto que $c = c \cdot 1$.

Si $c = ka$ y $c = mb$, entonces c es un *múltiplo común* de a y b. Si c es un múltiplo común positivo de a y b y todo otro común múltiplo d de a y b es múltiplo de c, entonces c *es el minimum común múltiplo* de a y b, y se escribe $c = [a, b]$. Del mismo modo, para cualquier conjunto finito de enteros a_1, a_2, $\ldots$, a_n que no sean todos cero, se puede determinar un mínimum común múltiplo positivo único $c = [a_1, a_2, \ldots, a_n]$ que tenga la propiedad de que todos los múltiplos comunes del conjunto sean múltiplos de c.

Se dice que dos enteros a y b son *primos entre sí* si todos sus divisores comunes son iguales a la unidad, es decir, $(a, b) = 1$. Por ejemplo, $(3, 4) = 1$; $(6,17) = 1$; $(64, 81) = 1$.

Consignamos las definiciones anteriores de términos tan familiares con el objeto de mantener nuestro pensamiento riguroso y también para que sirvan de base para consideraciones posteriores. En la sección que sigue de este capítulo examinaremos una pro-

piedad, menos familiar pero muy fundamental de los números enteros.

EJERCICIOS

1. Demostrar que si $a|b$, entonces $a|bc$ en donde c es un entero cualquiera.

2. Demostrar que si $a|b$, $a|c$, y $a|d$, entonces $a|(bx + cy - dz)$, en que x, y, z son enteros cualesquiera.

3. Demostrar que si $0 < a < b$, entonces b no es divisor de a.

4. Encontrar todos los enteros positivos N tales que todo entero positivo $n \leqq \sqrt{N}$ sea divisor de N.

5. Demostrar (a) que el conjunto de los números enteros pares forma un anillo y (b) que el conjunto de los enteros impares no forma un anillo. ¿Forma también, el conjunto de los enteros pares, un dominio de integridad?

6. Un número "perfecto" suele definirse como aquél que es igual a la suma de sus divisores positivos (excluidos el mismo número). Encontrar los primeros dos de estos números.

7. Demostrar que la suma de los cuadrados de dos enteros impares no puede ser el cuadrado de un entero.

8. Hacer los Ejercicios 1 a 4 del Capítulo I-18.

9. Determinar cuáles de los conjuntos de números del Ejercicio 1, Cap. I-14, forman dominios de integridad.

II·2 EL ALGORITMO DE LA DIVISION. Esta propiedad básica del conjunto de los enteros positivos se enuncia comúnmente como un teorema:

Si a y b son dos enteros positivos cualesquiera, existen enteros q y r, $0 \leqq q$, $0 \leqq r < a$ tales que $b = qa + r$.

Dados dos enteros positivos 1459 y 112, podríamos efectuar una división y escribir $1459 = 13 \cdot 112 + 3$. El teorema anterior simplemente establece que este uso de la división es una consecuencia lógica de nuestras definiciones y teoremas anteriores. Por eso el Algoritmo de la División, como mucho de nuestros otros teoremas, sirve para establecer un procedimiento aritmético común basado sobre el desarrollo de nuestro sistema de números que aparece en el Capítulo I.

Hay una "demostración" muy corriente del Algoritmo de la División que establece que, o bien $b = qa$, y en este caso $r = 0$, o bien, $b \neq qa$ y existe un entero q tal que $qa < b < (q + 1)a$. Por

consiguiente, existe siempre un entero r, $0 \leqq r < a$, tal que $b = qa + r$. Tal "demostración" parece razonable porque se vale solamente de propiedades familiares de nuestro sistema de números, es decir, si b se divide por a por medio de la operación de la división, entonces o bien $b = qa$ o $b \neq qa$, y existe un entero q que deja un resto menor que a. Sin embargo, uno de los propósitos del estudio del sistema de números es comprender en forma acabada cuáles son las suposiciones o postulados básicos necesarios. Otro propósito es identificar una "demostración" que señale que el resultado deseado puede obtenerse basándose sobre las suposiciones y definiciones fundamentales y en teoremas demostrados previamente. En la "demostración" anterior se han descuidado dos puntos. Primero, dados dos enteros positivos a y b, ¿existe siempre un entero N tal que $Na > b$? Segundo, si existiera por lo menos un entero N que satisfaga esta relación, ¿existe un entero menor que tal entero, es decir, un entero R tal que $(R - 1)\, a \leqq b < Ra$? La primera pregunta puede formularse así: ¿satisfacen los números enteros positivos el Postulado de Arquímedes? Y la segunda: ¿son los números enteros positivos bien ordenados?

El *Postulado de Arquímedes* establece que:

Dados dos enteros positivos cualesquiera a y b, existe un entero N tal que $Na > b$.

Esta propiedad de los enteros puede explicarse como sigue, de acuerdo con nuestras definiciones anteriores: puesto que a es un entero positivo debe ser $a = 1$ o bien $a > 1$. Si $a = 1$, entonces $ab = b$; si $a > 1$, entonces según el Capítulo I - 6, $(a - 1) > 0$, $(a - 1)\, b > 0$, $ab - b > 0$ y $ab > b$. En los dos casos, $ab + a = a(b + 1) > b$ y existe un entero $N = b + 1$ tal que $Na > b$. Por consiguiente, no necesitamos aceptar el Postulado de Arquímedes como un postulado, ya que puede demostrarse como teorema basándose sobre definiciones anteriores.

Finalmente, se dice que un conjunto de elementos está *bien ordenado* (Ejercicio 6, Cap. I - 6) si todo subconjunto no vacío de él tiene un primer elemento. Los enteros positivos son bien ordenados con respecto a la magnitud, los enteros negativos no lo son, los números racionales positivos tampoco, como tampoco es ordenado el conjunto de los números racionales de la forma de $1/n$.

La demostración de que los enteros positivos son bien ordenados es la siguiente: Sea I un subconjunto arbitrario de los enteros positivos. Se presentan tres casos según que I contenga sólo un número finito de elementos, que contenga infinitos elementos pero sólo a un número finito de elementos distintos, o que contenga infinitos elementos distintos. Si I contiene sólo un número finito de elementos, entonces existe un elemento mínimo de I, puesto que los enteros positivos están ordenados linealmente y es posible comparar los diversos elementos de un conjunto finito. Si I contiene infinitos elementos pero sólo un número finito de elementos distintos, sea N un extremo superior de los números finitos de elementos distintos de I. Entonces todo elemento de I coincide con uno de los números 1, 2, 3, . . ., N. Sea F el subconjunto de 1, 2, 3, . . ., N elementos que coincida con los elementos distintos de I. Entonces F es un conjunto finito y tiene un primer elemento que es también primer elemento de I. Por ejemplo, sea I el conjunto 1, 3, 5, 7, 1, 3, 7, 1, 3, 7, . . . y $N = 10$. Todo elemento de I coincide con uno de los números 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. El conjunto F es 1, 3, 5, 7, y 1 es el primer elemento de F y de I. Si I contiene infinitos elementos distintos, sea N un elemento de I. Entonces divídase al conjunto I en dos subconjuntos I_1 e I_2, en los cuales aquellos elementos de I que sean menores que o iguales a N pertenezcan a I_1 y de modo que todos los demás elementos pertenezcan a I_2. El conjunto I_1 está limitado y tiene un elemento mínimo, llamémoslo R. Puesto que R es menor que o igual a N, también es menor que todos los elementos de I_2 y es un elemento mínimo de I.

Ahora ya hemos examinado en detalle las suposiciones que sustenta la breve "demostración" del Algoritmo de la División. Hemos descubierto que las propiedades que se suponían para los números enteros pudieron demostrarse directamente basándose sobre las suposiciones y definiciones formuladas en el Capítulo I.

El Algoritmo de la División nos será muy útil. Desde un punto de vista práctico sirve de fundamento para la representación en base 10 de todos los números de nuestra notación decimal o indoarábica (Cap. II - 7). También se presta para un procedimiento, el Algoritmo de Euclides, empleado para encontrar el mayor divisor común de dos enteros cualesquiera (Cap. II - 5) o de dos polinomios cualesquiera en una variable (Cap. III - 7).

Consideraremos en seguida los números primos y estableceremos

las bases para un estudio acabado de los divisores o factores de cualquier entero dado que servirá como preparación para el Teorema de la Factorización Unica (Teorema II - 8).

EJERCICIOS

1. Demostrar que q y r son únicos en la relación $b = qa + r$ del Algoritmo de la División.

(Indicación: supóngase que $b = q_1a + r_1 = q_2a + r_2$ en donde $q_1 \geqq q_2$ y demuéstrese que $-a < r_2 - r_1 < a$).

2. Formule y demuestre el Postulado de Arquímedes respecto de dos números racionales cualesquiera.

3. ¿Qué propiedades debe tener un conjunto de elementos tales como 1, a, x, 5, r, 2, -1, . . . antes de que se intente demostrar que sus elementos satisfacen el Postulado de Arquímedes?

4. Señalar cuáles de los conjuntos de elementos siguientes están bien ordenados cuando se los ordena respecto a la magnitud: (a) los enteros mayores de 500, (b) los enteros mayores de -100, (c) enteros negativos, (d) números de la forma nk en que k es un número positivo dado y n es cualquier entero positivo, (e) los números racionales positivos, (f) los números irracionales positivos, (g) los números algebraicos.

5. Demostrar que los elementos de cualquier conjunto de elementos finito o numerable infinito puede ordenarse de modo que el conjunto sea bien ordenado.

6. Aprovechar el resultado del Ejercicio 5 y describir una ordenación de los números racionales de modo que el conjunto esté bien ordenado.

7. Demostrar que todo conjunto bien ordenado está ordenado linealmente (Cap. I-6).

II - 3 NUMEROS PRIMOS. La clasificación que sigue de los enteros de acuerdo con los múltiplos que ellos tienen o de acuerdo con los números por los cuales son divisibles, facilitará grandemente nuestro estudio. Ya se ha definido a cero como el elemento de identidad con respecto a la adición (Cap. I - 5). Los enteros $+1$ y -1 se llaman unidades (Cap. II - 1). Se dice que un entero p que no es cero ni una unidad es *primo* si sus únicos divisores son $\pm p$ y las unidades. Un entero se llama *compuesto* si tiene dos o más divisores primos (no necesariamente distintos). Por ejemplo $6 = 2 \cdot 3$ y $121 = 11^2$ son números compuestos. Todos los numeros enteros pertenecen a una de estas cuatro clases: cero, unidades, primos y números compuestos. Puesto que cero no es positivo ni negativo, esto significa que todo entero positivo perte-

nece a una de las tres clases restantes y que cada entero positivo mayor que uno es primo o compuesto. En el estudio siguiente se supone que los números primos negativos se expresan en la forma ep, en que e es la unidad -1 y p es un número primo positivo. De esta manera basta con considerar únicamente a los números primos positivos.

Usaremos estas definiciones en las demostraciones de varios teoremas.

TEOREMA II - 2. *Todo entero mayor que la unidad tiene un divisor primo positivo.*

Sea m cualquier entero dado mayor que la unidad. Entonces m es primo si y sólo si sus únicos divisores positivos son m y 1. Si m no es un número primo, tiene un divisor positivo m_1, en donde $m_1 \neq m$ y $m_1 \neq 1$. Por eso, si m no es primo, puede escribirse como el producto de dos enteros positivos, $m = m_1 m_2$, en que ni m_1 ni m_2 son iguales a la unidad. Si ni m_1 ni m_2 son primos, entonces $m = m_{11}m_{12}m_{21}m_{22}$ en que ningún m_{ij} es igual a la unidad. Si ningún m_{ij} es primo, entonces $m = m_{111}m_{112}m_{121}m_{122}m_{211}m_{212}m_{221}m_{222}$, en donde ningún m_{ijk} es la unidad. Este proceso termina si y sólo si en alguna etapa, por lo menos, uno de los m es un número primo. Demostraremos en seguida que, para cualquier entero positivo dado m el proceso debe terminar y no puede continuar indefinidamente. Primero, se observará que cualquier entero positivo m_2 que no sea la unidad satisface la relación de orden $m_2 > 1$ (Cap. I-6). Entonces se tiene también $m = m_1 m_2 > m_1$ y, en general,

$$m > m_1 > m_{11} > m_{111} > \cdots$$

para tantas etapas como las que tenga el proceso. Por consiguiente, el proceso termina si y sólo si el conjunto de enteros positivos $m, m_1, m_{11}, m_{111}, \ldots$ es un conjunto finito. En todo caso, este conjunto es un subconjunto del conjunto finito, $m, m-1, m-2, \ldots, 3, 2, 1$, y, por lo tanto, debe él mismo ser finito. De esta manera, el proceso en referencia debe terminar después de un número finito de etapas, y m debe tener un divisor primo.

También hemos demostrado que cualquier entero positivo dado m puede tener solamente un número finito de divisores enteros

positivos mayores que la unidad. El teorema siguiente indica cuáles son los enteros positivos que hay que considerar cuando se buscan los divisores positivos de un entero dado m.

TEOREMA II-3. *Si un entero positivo m es compuesto, entonces tiene un divisor primo positivo $\leqq I$, en donde I es el entero mayor cuyo cuadrado es $\leqq m$.*

Según el Teorema II-2, cualquier entero positivo m mayor que 1 tiene un divisor primo positivo p, es decir, $m = pm_1$. También si $m \neq p$, entonces m_1 tiene un divisor primo positivo $\leqq m_1$. Si el Teorema II-3 fuera falso, existiría un número m que fuera compuesto y no tuviera ningún divisor primo positivo $\leqq I$. En este caso, tendríamos $I < p, I < m_1$ o $I + 1 \leqq p, I + 1 \leqq m_1$ y $(I + 1)^2 \leqq pm_1 = m$, lo que es contrario a la suposición de que I es el entero mayor cuyo cuadrado es $\leqq m$. Por consiguiente, el Teorema II-3 debe ser verdadero (método de demostración indirecta, Cap. I-10).

Antes de que podamos aplicar el Teorema II-3 para determinar si un entero dado m, por ejemplo 359, es o no primo, necesitamos algún método para determinar los números primos $\leqq I$ en que $I^2 \leqq m < (I + 1)^2$. Para el caso de $m = 359$ necesitamos conocer los números primos $\leqq 18$.

Los números primos limitados por cualquier entero finito N pueden encontrarse por un método llamado la *Criba de Eratóstenes,* que es el siguiente: se escriben los enteros desde 1 hasta N, excluyendo el 1 puesto que es la unidad, contando a partir de 2 (se excluye el dos), tachar todos los segundos números de ahí en adelante; contando desde 3 (excluido el 3), tachar todos los terceros números de ahí en adelante, y, en general, contando desde cualquier entero k que es $\leqq \sqrt{N}$ (Teorema II-3), tachar todos los enteros de orden k. Por ejemplo, los números primos limitados por $N = 18$ son 2, 3, 5, 7, 11, 13, 17, y pudieron encontrarse del siguiente esquema:

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~,

en el cual fue sólo necesario excluir la unidad y los múltiplos de 2 y 3 ya que el entero siguiente que quedaba, 5, tiene un cuadrado mayor que 18.

Después de esto, podemos usar el Teorema II-3 y determinar si 359 es primo o no, probando sucesivamente si 359 es divisible por 2, 3, 5, 7, 11, 13, 17. Sobre esta base podemos aseverar que 359 es un número primo.

Una de las razones para considerar métodos mecánicos como el anterior para determinar números primos es que aún no se ha encontrado ninguna fórmula ni representación analítica para los números primos. Sin embargo, podremos demostrar varios teoremas referentes a los números primos. El teorema siguiente es una versión moderna de la Proposición 20 del Libro IX de los *Elementos* de Euclides.

TEOREMA II-4. *El conjunto de los números primos positivos es infinito numerable.*

Supongamos que hubiera un número primo mayor que todos los demás, por ejemplo, P, entonces $N = P! + 1$ debe tener un divisor primo (Teorema II-2). Pero ningún número $\leqq P$ es divisor de $P! + 1 = N$. Por eso, N tiene un divisor primo mayor que P y no hay ningún primo mayor que todos los demás, es decir, el conjunto de los números primos positivos es infinito numerable. Por ejemplo, si $P = 2$, entonces $N = 2! + 1 = 3$, que es primo; si $P = 5$, entonces, $N = 5! + 1 = 121$, que tiene a $11 > 5$ como divisor primo. Este procedimiento para determinar la existencia de un número primo mayor que cualquier número primo dado P, puede aprovecharse también, junto con el hecho de que existe un solo número primo 2, para demostrar por inducción matemática (Cap. I-4) que existe un subconjunto infinito numerable del conjunto de los números primos positivos. Luego, puesto que el conjunto de todos los números primos positivos es un subconjunto del conjunto de los enteros positivos, que es infinito numerable, hemos obtenido otra demostración de que el conjunto de los números primos positivos es infinito numerable.

Las propiedades más conocidas de los números primos se refieren a la divisibilidad. Dado cualquier entero m y el número primo p, los únicos divisores positivos de p, y, por lo tanto, los únicos comunes divisores positivos posibles de p y m, son p y 1. De aquí que resulte el

TEOREMA II-5. *Si p es un número primo y m es cualquier número entero, entonces p es un divisor de m o bien $(p, m) = 1$.*

Otro teorema conocido puede demostrarse como sigue: Supongamos que p es un número primo, y a y b sean cada uno enteros positivos menores que p. Deseamos demostrar que p no es divisor del producto ab, y se escribe $p \nmid ab$. Nos valdremos del método de demostración indirecta y supondremos que $p \mid ab$. Además, supondremos que b es el entero positivo menor tal que $p \mid ab$, es decir, ab es el múltiplo menor de a tal que $p \mid ab$. Esta última suposición puede hacerse sin perder la generalidad de la demostración, ya que si existe un múltiplo entero único, éste debe ser el múltiplo entero positivo menor de a que sea divisible por p (Cap. II-2). Ahora bien, según el Algoritmo de la División, existe un entero m tal que,

$$mb \leqq p < (m + 1)b, 0 \leqq p - mb < b.$$

En realidad, $mb \neq p$ puesto que $1 < b < p$ y p es primo. Por *suposición*, $p|ab$ y también $p|mab$. Entonces de $p|ap$ se tiene $p|(ap - mab)$ y $p|a(p - mb)$, de donde $a(p - mb)$ es un múltiplo de a que es divisible por p. Pero también $a(p - mb) < ab$, lo que es contrario a la suposición de que ab sea el menor múltiplo de a que es divisible por p. Por consiguiente, p no es divisor de ab, y hemos hecho una demostración indirecta del siguiente teorema:

TEOREMA II - 6. *Si p es un número primo, y a y b son dos enteros positivos, cada uno menor que p, entonces $p \nmid ab$.*

Este teorema puede ampliarse para dos enteros positivos cualesquiera a y b tales que $p \nmid a$ y $p \nmid b$. Sea $a = mp + r$, $b = np + s$, $0 < r < p$, $0 < s < p$. Ahora bien, si $p|ab$, tenemos también $p|rs$, lo que es contrario al Teorema II-6. Por consiguiente, si $p \nmid a$ y $p \nmid b$, entonces $p \nmid ab$. En otras palabras, si $p|ab$, entonces se verifica que $p|a$ o bien $p|b$. Puesto que el producto de dos enteros es un entero, también podemos hacer $a_1 \cdot a_2 = a$, $a_3 = b$ y demostrar que si $p|a_1a_2a_3$, entonces p es divisor de por lo menos uno de los números a_1, a_2, a_3. Por aplicación repetida de este procedimiento, tenemos

TEOREMA II-7. *Si p es un número primo y $p | a_1 a_2, \ldots a_n$, entonces p es divisor de por lo menos uno de los enteros $a_1, a_2, \ldots, a_n$, en donde n es un entero positivo cualquiera.*

Una aplicación muy importante de esta propiedad de los números primos se encuentra en la factorización de todos los enteros positivos como productos de potencias de números primos (Cap. II - 4). En todo el resto de este libro usaremos ampliamente las propiedades de los números primos y las propiedades análogas de los polinomios irreducibles (Cap. III - 6).

EJERCICIOS

1. Encontrar los números primos menores que 200, por medio de la Criba de Eratóstenes.

2. Determinar cuáles de los números siguientes son primos:

a) 85, 103, 179, 539;

b) 267, 781, 859, 937;

c) 1245, 2287.

3. Escribir una demostración rigurosa del Teorema II-7 por medio de la inducción matemática.

4. ¿Es $n^2 - n + 41$ un número primo para todos los valores enteros positivos de n? Explicar

5. Dar cuatro ejemplos numéricos para ilustrar el Teorema II-5.

6. Repetir el Ejercicio 5 para los Teoremas II-6 y II-7.

7. Dado un entero N cualquiera, ¿cómo se pueden encontrar *todos* sus divisores primos positivos?

8. Demostrar que $n^3 + 1$ es un número compuesto si n es mayor que la unidad.

9. Demostrar que $3^n - 1$ y en general, $m^n - 1$ es un número compuesto si n es mayor que uno y m es mayor que 2 (ver Ejercicio 7, Cap. I-4).

10. Un número de la forma $2^p - 1$ que sea primo se llama *número primo de Mersenne*. Encontrar cinco números de éstos.

11. Demostrar que $2^n - 1$ es un número compuesto si n es compuesto. (Ver Ejercicio 9, Cap. I-4). Dar un ejemplo de un número compuesto de la forma $2^p - 1$ en que p sea un número primo.

II-4 TEOREMA DE LA FACTORIZACION UNICA. Se dice que un entero se ha factorizado completamente cuando se ha expresado como producto de números primos (positivos) y una unidad ($+1$ o -1). En esta

sección del Cap. II tendremos en cuenta, primero, que el producto de cualquier número finito de unidades es una unidad y demostraremos que cualquier entero puede expresarse como un producto de números primos positivos y una unidad de una manera única. En seguida deduciremos algunas consecuencias más de esta factorización.

El entero positivo 168 puede expresarse como un producto de enteros de diversas maneras. Por ejemplo,

$$168 = 4 \cdot 42 = 2 \cdot (-2) \cdot (-7) \cdot 6 = 21 \cdot 8 = 7 \cdot 24.$$

El teorema de la factorización única establece que si 168 se expresa como producto de números primos positivos, $168 = 2^3 \cdot 3 \cdot 7$, cualquiera otra factorización en divisores primos tal como $168 = 3 \cdot 2^3 \cdot 7$, debe coincidir con la primera, salvo por el orden en que están escritos los divisores.

Cualquier entero positivo m mayor que 1 tiene por lo menos un divisor o factor primo positivo según el Teorema II - 2. Este divisor primo, sea p_1, puede hallarse en un número finito de etapas, puesto que m es finito y p_1 es uno de los números 1, 2, 3, ..., m. Si $p_1 = m$, nuestra factorización es completa y es única. Si $p_1 \neq m$, entonces $m = p_1 m_1$ y si procedemos como anteriormente con m_1, obtendremos $m = p_1(p_2 m_2)$ si m_1 no es primo. Ya que los enteros positivos $m, m_1, m_2, \ldots$ satisfacen la relación $m > m_1 > m_2 > \ldots$, el proceso anterior, lo mismo que aquél de la demostración del Teorema II-2, debe terminar después de un número finito de pasos y resultar

(II - 1) $$m = p_1 p_2 \ldots p_r.$$

Si hubiera también una segunda factorización,

(II - 2) $$m = q_1 q_2 \ldots q_s$$

de m en divisores primos positivos, tendríamos

(II - 3) $$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Puesto que p_1 es divisor de $q_1 q_2 \ldots q_s$, debe, según el Teorema II - 7, ser divisor de algún q_i, sea q_1. Ya que hemos aceptado que

q_1 y p_1 son números primos positivos, $p_1 = q_1$. Dividimos entonces ambos miembros de (II - 2) por $p_1 = q_1$ y repetimos el mismo argumento para demostrar que p_2 es igual a alguno de los números q, sea q_2. Este proceso puede continuarse hasta que uno de los miembros de (II - 3) quede reducido a 1. Puesto que los números p y q son enteros, el otro miembro debe simultáneamente hacerse igual a 1. De aquí que exista una factorización de m en divisores primos, y si se presentan dos factorizaciones (II - 1) y (II - 2) de m en divisores primos, éstas son idénticas, excepto posiblemente en el orden en que están escritos los divisores. Por consiguiente, los divisores y la factorización son únicos. Si los números primos iguales se agrupan juntos, tenemos el *Teorema de Factorización Unica* o, como suele llamarse, el *Teorema Fundamental de la Aritmética:*

TEOREMA II - 8. *Todo entero con la excepción de cero puede representarse de una y sólo una manera en la forma*

$$m = e_j p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n},$$

en que e_j *es una de las unidades, los* p_i *son números primos positivos distintos y los* a_i *son enteros positivos.*

Por lo tanto, dado cualquier entero m, podemos elegir la unidad adecuada y entonces aplicar el Teorema II - 3 y divisiones sucesivas para encontrar los divisores primos positivos de m. Por ejemplo,

$$12 = 2^2 \cdot 3; \; -36 = (-1) \cdot 2^2 \cdot 3^2; \; 1232 = 2^4 \cdot 7 \cdot 11.$$

Examinemos por un momento $12 = 2^2 \cdot 3$. Cualquier divisor primo de 12 debe ser divisor de 2^2 ó de 3, según el Teorema II-7. Por consiguiente, 2 y 3 son los únicos divisores primos de 12. Asimismo, todos los divisores positivos de 12 pueden expresarse en la forma $d = 2^a \cdot 3^b$, en donde $a = 0, 1, 2$ y $b = 0$ ó 1. Todos los divisores de 12 tienen la forma $e \cdot 2^a \cdot 3^b$, en donde e es una unidad, $0 \leqq a \leqq 2$, y $0 \leqq b \leqq 1$. En general, todos los divisores de $m =$

$e_j p_1^{a_1} p_2^{a_2} \ldots\ldots p_n^{a_n}$ son de la forma

(II - 4) $\qquad e_k p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$, en que $0 \leqq b_i \leqq a_i$

y e_i es una unidad. Además, todo número de la forma (II - 4) es un divisor de m. De este concepto de divisor y del Teorema II - 8 se desprende que

TEOREMA II-9. *Si a y b no tienen divisores comunes y cada uno de ellos es divisor de c, entonces su producto es divisor de c. Si a y c no tienen divisores comunes y b y c no tienen divisores comunes, entonces ab y c no tienen divisores comunes. Si a y c no tienen divisores comunes y c es divisor de ab entonces c es divisor de b.*

Las tres partes de este teorema se pueden expresar matemáticamente como sigue: (i) $(a,b) = 1$, $a|c$ y $b|c$ implica $ab|c$; (ii) $(a, c) = 1$ y $(b, c) = 1$ implica $(ab, c) = 1$; (*iii*) $(a, c) = 1$ y $c|ab$ implica $c|b$. Las demostraciones de estos enunciados se dan como ejercicios (Ejercicios 3, 4 y 5).

El Teorema II - 8 puede también usarse para encontrar el máximo común divisor y el mínimo común múltiplo de dos enteros (Cap. II - I). Por ejemplo, si $m = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$ y $n = 2^2 \cdot 3^3 \cdot 7^2 \cdot 11$, entonces $(m,n) = 2^2 \cdot 3^2 \cdot 7$ y $[m,n] = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$. Estos valores particulares pueden obtenerse a la simple vista. En general, suele ser ventajoso expresar m y n por medio de los mismos números primos positivos, empleando para esto el exponente cero. Por ejemplo, en el caso anterior, $m = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11^0$ y $n = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11$. Por eso, dados dos enteros cualesquiera m y n, se puede escribir cada uno de ellos por medio de sus divisores primos positivos y en seguida expresar cada cual, como anteriormente, mediante el mismo conjunto de números primos, es decir, $m = e_j p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ y $n = e_r p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$. Estas expresiones pueden abreviarse valiéndose del símbolo para el producto $\prod$, como sigue

$$m = e_j \prod_{i=1}^{k} p_i^{a_i}, \quad n = e_r \prod_{i=1}^{k} p_i^{b_i}.$$

Entonces (m,n) se obtiene tomando el menor exponente que se presente en cada número primo p_i, y $[m,n]$ se obtiene tomando el mayor exponente que aparezca en cada número primo p_i. La nota-

ción matemática sería $(m, n) = \prod_{i=1}^{k} p_i^{c_i}$, $[m, n] = \prod_{i=1}^{k} p_i^{d_i}$,
en donde c_i, es el mínimum de a_i y b_i; y d_i es el máximum de a_i y b_i.

Finalmente, supongamos $(a, b) = d$, $[a, b] = m$, y sea $a = a_1d$, $b = b_1d$. Entonces $(a_1, b_1) = 1$, el mínimo común múltiplo de a y b es $m = a_1b_1d$, y $dm = da_1b_1d = ab$. De este modo tenemos

TEOREMA II-10. *Si a y b son enteros positivos, $(a, b) = d$, y $[a, b] = m$, entonces $dm = ab$.*

Por ejemplo, $(6, 8) = 2$, $[6, 8] = 24$, y $6 \cdot 8 = 2 \cdot 24$. El hecho de que este teorema no pueda aplicarse directamente para el caso de tres enteros positivos se evidencia en el ejemplo siguiente: $(6, 4, 10) = 2$; $[6, 4, 10] = 60$, y $6 \cdot 4 \cdot 10 = 240 \neq 2 \cdot 60$.

En la sección que sigue de este capítulo nos serviremos del Algoritmo de Euclides para encontrar $d = (a, b)$ sin tener que expresar primeramente a y b por medio de sus divisores primos. En seguida por medio de la expresión $m = ab|d$ del Teorema II - 10 encontraremos $m = [a, b]$. Es así como luego podremos encontrar (a, b) y $[a, b]$ sin necesidad de expresar a y b en sus divisores primos.

EJERCICIOS

1. Descomponer en sus divisores primos positivos los números 4680, 1275 y 1278.
2. Encontrar (4680, 1275) y [4680, 1275] por medio de sus divisores primos. ¿Es válido el Teorema II-10 para este caso?
3. Demostrar la primera parte del Teorema II-9.
4. Demostrar la segunda parte del Teorema II-9.
5. Demostrar la tercera parte del Teorema II-9.
6. Dado cualquier entero n ¿cómo se pueden encontrar *todos* sus divisores positivos?
7. Encontrar todos los divisores positivos de 60.
8. Demostrar que todo divisor positivo de $m = e_1p_1^{a_1}p_2^{a_2}\dots p_n^{a_n}$ aparece una vez y sólo una entre los términos del producto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{a_1})(1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots (1 + p_n + p_n^2 + \cdots + p_n^{a_n}).$$

9. Demostrar que el entero m en el Ejercicio 8 tiene $(a_1 + 1)(a_2 + 1) \ldots (a_n + 1)$ divisores positivos distintos.

10. Demostrar que la suma de los divisores positivos del entero m en el Ejercicio 8 puede expresarse en la forma

$$\prod_{i=1}^{n} \frac{p_i^{a_i+1} - 1}{p_i - 1},$$

por medio del símbolo del producto $\prod$.

11. Determinar cuántos son y cuánto suman los divisores positivos de 60, por medio de los Ejercicios 9 y 10.

12. ¿Cuántos divisores tiene cada uno de los números del Ejercicio 1?

13. Encontrar la suma de los divisores de cada uno de los números del Ejercicio 1.

II - 5 EL ALGORITMO DE EUCLIDES.

En el Cap. II - 4 se expresó el máximo común divisor (m, n) de dos enteros por medio de los divisores primos de los dos enteros. El Algoritmo de Euclides proporciona un método directo para obtener el máximo común divisor de dos enteros sin tener que expresar los enteros en sus divisores primos. Este método es ventajoso especialmente cuando se trata de números grandes. En el caso de 36 y 90, el método del Cap. II - 4 se escribiría $36 = 2^2 \cdot 3^2$ y $90 = 2 \cdot 3^2 \cdot 5$, luego $(36, 90) = 2 \cdot 3^2 = 18$. El Algoritmo de Euclides daría $90 = 2 \cdot 36 + 18$; $36 = 2 \cdot 18 + 0$; y $(36, 90) = 18$.

En general, como el máximo común divisor se considera positivo, se puede calcular para dos enteros cualesquiera diferentes de cero, tomando en cuenta sólo los enteros positivos correspondientes m, n cada vez que se presenten los factores $+1$ o -1. Si $m = n$, entonces también $(m, n) = m$; si $m \neq n$, supongamos que $m > n$. Entonces aplicamos el Algoritmo de la División repetidas veces (Cap. II - 2) y obtenemos el *Algoritmo de Euclides:*

$$\begin{array}{lll}
(2\text{-}5) & m = qn + n_1, & 0 < n_1 < n \\
(2\text{-}6) & n = q_1 n_1 + n_2, & 0 < n_2 < n_1 \\
(2\text{-}7) & n_1 = q_2 n_2 + n_3, & 0 < n_3 < n_2 \\
 & \cdot & \cdot \\
 & \cdot & \cdot \\
 & \cdot & \cdot \\
(2\text{-}8) & n_{k-2} = q_{k-1} n_{k-1} + n_k, & 0 < n_k < n_{k-1} \\
(2\text{-}9) & n_{k-1} = q_k n_k. & 0 = n_{k+1}
\end{array}$$

Puesto que los enteros n, n_1, n_2, ... forman una sucesión decreciente, es decir, $n > n_1 > n_2 > \ldots$, existe algún entero n_j, sea n_{k+1}, igual a cero y tal que $k = 0$ o bien n_k sea diferente de cero. Encontraremos que cuando $k = 0$ $(m,n) = n = n_0$; y cuando $k \neq 0$, $(m,n) = n_k$.

Cualquier divisor común de m y n, debe ser divisor de n_1 de acuerdo con la relación (II - 5); debe ser divisor de n_2 de acuerdo con (II - 6); de n_3 de acuerdo con (II - 7), ..., y de n_k de acuerdo con (II - 8). De este modo, todo divisor común de m y n es divisor de n_k. Inversamente, n_k es divisor de n_{k-1} de acuerdo con (II - 9); de n_{k-2} de acuerdo con (II - 8), ..., de n_1 de acuerdo con (II - 7); de n de acuerdo con (II - 6); y de m de acuerdo con (II - 5), es decir, n_k es un divisor común de m y de n. Estos resultados se enuncian en el siguiente teorema:

TEOREMA II-11. *El máximo común divisor de dos enteros positivos cualesquiera m y n puede encontrarse por medio del Algoritmo de Euclides: es el último resto que no desaparece. Existen enteros A y B tales que*

$$(m,n) = n_k = Am + Bn. \qquad \text{(II - 10)}$$

Los enteros A y B de (II - 10) se pueden obtener resolviendo (II - 5) para n_1 en la fórmula $n_1 = A_1m + B_1n$ y sustituyendo esto en (II - 6) para obtener $n_2 = A_2m + B_2n$, ... : finalmente $n_k = Am + Bn$ se obtiene de (II - 8). Por ejemplo, tenemos la forma siguiente del Algoritmo de Euclides para los números 23 y 19:

$$\begin{aligned} 23 &= 1 \cdot 19 + 4, \\ 19 &= 4 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0, \end{aligned}$$

de donde $(23, 19) = 1$. Puede encontrarse una relación de la forma (II - 10) que se indica anteriormente, por medio de las ecuaciones

$$\begin{aligned} 4 &= 1 \cdot 23 - 1 \cdot 19, \\ 3 &= 1 \cdot 19 - 4 \cdot 4 = 5 \cdot 19 - 4 \cdot 23, \\ 1 &= 1 \cdot 4 - 1 \cdot 3 = 5 \cdot 23 - 6 \cdot 19. \end{aligned}$$

Este procedimiento puede expresarse por medio de los cuocientes generales q_j y restos n_j desde (II - 5) hasta (II - 9) de la manera siguiente:

$$
\begin{aligned}
n_1 &= m - qn = A_1m + B_1n,\\
n_2 &= -q_1m + (q_1q + 1)n = A_2m + B_2n,\\
n_3 &= (q_1q_2 + 1)m - (q_2 + qq_1q_2 + q)n = A_3m + B_3n,\\
&\;\;\vdots
\end{aligned}
$$

Los coeficientes de m y n son enteros en todas las etapas, ya que únicamente se trata de las operaciones del anillo: la adición, la sustracción y la multiplicación.

Queda aún el problema práctico de encontrar A y B para enteros cualesquiera dados m y n con el menor trabajo posible. Para cualquier entero $m \neq 0$, tenemos $(m, 0) = em$ en donde e es una unidad. También hemos hecho notar que se puede suponer que los enteros dados son positivos sin que se pierda la generalidad de la expresión. El esquema siguiente proporciona un procedimiento práctico para determinar el máximo común divisor y una relación de la forma (II - 10) para dos enteros positivos cualesquiera m y n. Los números n_j y q_j son los mismos que los de (II - 5) hasta (II - 9). El esquema

$$
\text{(2-11)}\qquad
\begin{array}{cccccccc}
m & n & n_1 & n_2 & n_3 & \ldots & n_k & 0\\
 & q & q_1 & q_2 & q_3 & \ldots & q_k & \\
 & 1 & -q & B_2 & B_3 & \ldots & B_k = B & \\
 & & 1 & -q_1 & A_3 & \ldots & A_k = A &
\end{array}
$$

puede construirse por medio del diseño geométrico

$$
\begin{array}{ccc}
n_{i-1} & n_i & n_{i+1}\\
 & q_i &
\end{array}
$$

en las primeras dos filas para significar que $n_{i-1} = q_in_i + n_{i+1}$; representando el último n_j diferente de cero por n_k, y determinando los A_j y B_j por medio de las fórmulas de recurrencia

$$B_0 = 1,\ A_0 = 0,\ B_1 = -q,\ A_1 = 1,$$
$$\begin{aligned} B_{i+1} &= B_{i-1} - q_iB_i, \\ A_{i+1} &= A_{i-1} - q_iA_i. \end{aligned} \qquad (i = 1, 2, 3, 4, \ldots, k-1)$$

Para el caso de $m = 23$, $n = 19$, este esquema resulta ser

	23	19	4	3	1	0
(II - 12)		1	4	1	3	
		1	—1	5	—6	
			1	—4	5	

de donde $(23, 19) = 1$ y $1 = 5 \cdot 23 - 6 \cdot 19$, tal como se obtuvo anteriormente.

El método anterior para obtener n_k es simplemente una representación sintética de las relaciones (II - 5) a (II - 9) y por lo tanto es válido. El método anterior para determinar A_k y B_k puede verificarse por inducción matemática respecto de j, en donde $n_j = mA_j + nB_j$. Para $j = 0$, se hace $n_0 = n$ y se tiene $n = n$; para $j = 1$ se tiene $n_1 = m - qn$, que es válido según (II - 5). Supongamos que $n_{i-1} = mA_{i-1} + nB_{i-1}$ y que $n_i = mA_i + nB_i$, entonces

$$\begin{aligned} n_{i+1} &= n_{i-1} - q_in_i \\ &= m(A_{i-1} - q_iA_i) + n(B_{i-1} - q_iB_i) \\ &= mA_{i+1} + nB_{i+1}, \end{aligned}$$

y se verifican así las fórmulas de recurrencia dadas más arriba.

El método representado por el esquema (II - 11) puede ser muy útil después de un poco de práctica. Es ventajoso especialmente porque el máximo común divisor puede determinarse sólo por medio de las dos primeras filas. Luego, si se desea una relación de la forma (II - 10), se pueden determinar las constantes A y B.

La ecuación (II - 10) es, pues, necesaria y suficiente para que n_k sea el máximo común divisor de m y n. Es necesaria según el Teorema II - 11 y es suficiente ya que si (II - 10) es válido, todo factor común de m y n debe ser divisor de n_k. Como una aplicación particular de esto, tenemos

TEOREMA II - 12. *Dos enteros m y n son primos entre sí si y sólo si hay enteros A y B tales que* $Am + Bn = 1$.

Nos serviremos del Algoritmo de Euclides y del Teorema II - 12 para obtener el recíproco de n, módulo m en la sección 11 de este Capítulo II. En el Cap. III - 7 estos resultados se formulan nuevamente para polinomios $p(x)$. En esta forma se emplearán para encontrar el máximo común divisor de dos polinomios, el número de raíces distintas de una ecuación polinomia en cualquier intervalo $a < x \leqq b$ (Cap. IV - 12), y las raíces múltiples de una ecuación polinomia (Cap. IV - 13).

EJERCICIOS

1. ¿Cómo se puede demostrar, mediante el Algoritmo de Euclides, la existencia de un máximo común divisor entre dos enteros positivos cualesquiera?

2. Demostrar que $(km, kn) = k(m, n)$ para cualquier entero positivo k.

3. Expresar cada uno de los siguientes divisores en la forma (II-10):

a) (108, 64),
b) (370, 111),
c) (147, 64),
d) (3961, 952),
e) (4680, 1275).

Comparar con el Ejercicio 2, Cap. II-4.

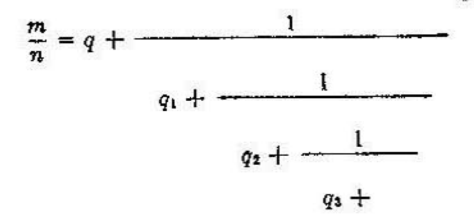
4. Encontrar el mínimo común múltiplo de cada uno de los pares de números del Ejercicio 3.

5. Demostrar que $[km, kn] = k[m, n]$.

6. Demostrar que si $(a, b) = 1$, en que a y b son enteros cualesquiera, entonces existen enteros d y e tales que

$$\frac{1}{ab} = \frac{d}{a} + \frac{e}{b}.$$

7. Demostrar que todo número racional positivo puede expresarse como una fracción continua finita de la forma



$$\cdots + \frac{1}{q_k}$$

que se suele escribir de la manera siguiente:

$$\frac{m}{n} = q + \frac{1}{q_1 +} \; \frac{1}{q_2 +} \; \frac{1}{q_3 +} \cdots + \frac{1}{q_k}.$$

(Indicación: Los q aquí son los mismos que en el Algoritmo de Euclides. La expresión que correspondería a (II - 12) sería

$$\frac{23}{19} = 1 + \frac{1}{4+} \; \frac{1}{1+} \; \frac{1}{3+}\,)$$

8. Aprovechese el resultado obtenido en el Ejercicio 3 y exprésese cada uno de los siguientes números racionales como fracciones continuas:

$$\frac{108}{64}, \frac{370}{111} \; \frac{147}{64}, \frac{3961}{952}, \frac{4680}{1275}.$$

9. Demostrar que $-B/A$ en (II-10) es una aproximación de m/n que difiere de m/n en n_k/An. Esta es una primera aproximación muy práctica y es equivalente a despreciar el término q_k en el Ejercicio 7. De consiguiente $\frac{23}{19}$ es aproximadamente $\frac{6}{5}$, y en este caso el error es de $\frac{1}{114}$.

10. Emplear el método del Ejercicio 9 y encontrar las primeras aproximaciones a cada una de las fracciones del Ejercicio 8. Indicar el error de la aproximación en cada caso.

11. Continuar el procedimiento de aproximación comenzado en el Ejercicio 9 y demostrar que en general la aproximación de orden $(j + 1)$ de m/n es $-B_{k-j}/A_{k-j}$ en la fórmula (II-11).

II - 6 BASES. El concepto de una "base" es tan fundamental en la teoría de los números como lo es en "baseball".

Cualquiera interpretación de un número, tal como 1776, en el cual la posición de los dígitos tiene un significado, depende del número particular que se ha elegido como base. Por ejemplo, 11 representa once en base diez, es decir, una decena y una unidad en la notación decimal. Sin embargo, 11 también representa tres en la base dos, es decir, un grupo de dos y una unidad en el sistema binario de números. Todos estamos familiarizados con la notación decimal (Cap. II - 7) que emplea la base diez y los dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. El sistema binario se sirve sólo de dos dígitos, que son 0 y 1, y ha alcanzado una importancia creciente con el desarrollo de los computadores electrónicos, puesto que sus dígitos pueden representarse por la presencia y ausencia, respectivamente, de una corriente eléctrica. En general, demostraremos que todo entero positivo n mayor que 1 puede usarse como base para todos los enteros positivos, es decir,

TEOREMA II - 13. *Si m y n son enteros positivos, y $n > 1$, entonces la representación*

$$m = a_k n^{k-1} + a_{k-1} n^{k-2} + \cdots + a_1$$

en donde $a_k \neq 0$, $0 \leqq a_i < n$ para $i = 1, 2, \ldots, k$, existe para algún entero k y es única.

Por ejemplo, el entero 130, puede expresarse en bases 10, 2, 3, 4, 5 y 6, como sigue:

II-13.
$$\begin{aligned}
130 &= 1 \cdot 10^2 + 3 \cdot 10 + 0 = 130_{10}, \\
130 &= 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4, \\
&\quad + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 0 = 10000010_2, \\
130 &= 1 \cdot 3^4 + 1 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3 + 1 = 11211_3, \\
130 &= 2 \cdot 4^3 + 0 \cdot 4^2 + 0 \cdot 4 + 2 = 2002_4, \\
130 &= 1 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 0 = 1010_5,
\end{aligned}$$

II-14.
$$130 = 3 \cdot 6^2 + 3 \cdot 6 + 4 = 334_6.$$

Los enteros a_i pueden encontrarse por medio de la aplicación repetida del Algoritmo de la División (Cap. II - 2), pero el procedimiento es completamente diferente del que se usó en el Cap. II - 5. Por ejemplo, en las expresiones anteriores (II - 13) y (II - 14), tenemos,

$$130 = 10 \cdot 13 + 0, \qquad 130 = 6 \cdot 21 + 4$$
$$13 = 10 \cdot 1 + 3, \qquad 21 = 6 \cdot 3 + 3,$$
$$1 = 10 \cdot 0 + 1, \qquad 3 = 6 \cdot 0 + 3.$$

Los restos sucesivos 0, 3, 1 cuando se divide 130 repetidas veces por 10, son las unidades, decenas y centenas representadas por los dígitos correspondientes, es decir, los coeficientes de 1, 10, y 10^2 en la fórmula (II - 13). Asimismo, los restos sucesivos 4, 3, 3 cuando 130 se divide reiteradamente por 6, son los coeficientes de 1, 6, y 6^2 en la expresión (II - 14). Estos coeficientes se obtienen fácilmente por medio de los siguientes esquemas donde los restos se separan a un lado:

10|180		6|130	
10|13	~0	6|21	~4
10|1	~3	6|3	~3
0	~1	0	~3

En general, el coeficiente a_i, del Teorema II - 13, puede obtenerse como sigue. Supongamos

$$\begin{aligned} m &= q_1 n + r_1, \\ q_1 &= q_2 n + r_2, \\ q_2 &= q_3 n + r_3, \\ &\cdots \\ q_{k-2} &= q_{k-1} n + r_{k-1}, \\ q_{k-1} &= 0 \cdot n + r_k, \end{aligned}$$

en donde $0 \leqq r_i < n$. De estas ecuaciones, se tienen $m > q_1 > q_2 > \cdots > q_{k-1} > 0$; $0 < q_{k-1} < n$; $r_k = q_{k-1}$, y por lo tanto $0 < r_k$. Los coeficientes del Teorema II - 13 se obtienen haciendo $a_k = r_k$, $a_{k-1} = r_{k-1}$, $\ldots$, $a_1 = r_1$.

Las relaciones $a_j = r_j$ pueden verificarse substituyendo cada q_i en la ecuación $q_{i-1} = q_i n + r_i$ para $i = k-1, k-2, \ldots, 2, 1$, y $q_0 = m$, como sigue:

$$q_{k-1} = r_k,$$
$$q_{k-2} = r_k n + r_{k-1},$$
$$q_{k-3} = r_k n^2 + r_{k-1} n + r_{k-2},$$
$$\cdot$$
$$\cdot$$
$$q_1 = r_k n^{k-2} + r_{k-1} n^{k-3} + \cdots + r_2,$$
$$m = r_k n^{k-1} + r_{k-1} n^{k-2} + \cdots + r_1.$$

Si hubiera dos expresiones para m en la misma base n, sean

$$m = a_0 n^k + a_1 n^{k-1} + \ldots + a_{k-1} n + a_k,\ 0 < a_0\ 0 \leqq a_k < n$$

y

$$m = b_0 n^p + b_1 n^{p-1} + \ldots + b_{p-1} n + b_p,\ 0 < b_0,\ 0 \leqq b_i < n,$$

entonces tendríamos

$$a_0 n^k + a_1 n^{k-1} + \ldots + a_k - (b_0 n^p + b_1 n^{p-1} + \ldots + b_p) = 0.$$

El miembro de la derecha, 0 (y por lo tanto el miembro de la izquierda de esta ecuación) es divisible por n. Por eso n es divisor de $a_k - b_p$. Pero

$$0 \leqq a_k < n,\ 0 \leqq b_p < n,\ |a_k - b_p| < n,$$

y n no es divisor de ningún entero positivo menor que n. Puesto que $|a_k - b_p|$ es divisible por n, no puede ser positivo y debe ser igual a 0, es decir, $a_k = b_p$. Asimismo, ambos miembros deben ser divisibles por n^{j+1}, de donde $a_{k-j} = b_{p-j}$ o, en general, $a_i = b_i$ para todos los valores de i, y tenemos que $p = k$. Por consiguiente la representación de m en el Teorema II - 13 es única.

La notación indo-arábica o sistema decimal (Cap. II-7) que nosotros usamos, consta de números expresados en base 10. En este caso el Teorema II - 3 establece que todo entero positivo tiene una representación única en base 10. Por ejemplo,

$$5604 = 5 \cdot 10^3 + 6 \cdot 10^2 + 0 \cdot 10 + 4.$$

Asimismo para $n = 2$ el Teorema II - 13 establece que todo entero positivo tiene una representación única en base 2. Por ejemplo,

$$183 = 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1,$$

y puede indicarse por 10110111_2. El sistema binario puede ampliarse de la misma manera que el sistema decimal para representar $7.625 = 1 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 2^0 + 1 \cdot 2^{-1} + 0 \cdot 2^{-2} + 1 \cdot 2^{-3}$ por 111.101_2. Sobre el sistema binario se basa la multiplicación campesina rusa, un antiguo método de convertir en suma la multiplicación de dos enteros (Ejercicios 11 y 12). Más recientemente, como se dijo antes, el sistema binario es la base de los cálculos con computadores electrónicos.

Hay muchos problemas y juegos que dependen de la escala de notación, es decir, de la base en la cual se expresan los números. Ball (Ver Bibliografía Nº 3; págs. 11 - 16) señala varios problemas en donde se utiliza la base 10. Por ejemplo, si una persona elige dos enteros menores que 10 (es posible al tirar dos dados), se puede descubrir cuáles son los enteros, pidiéndole lo siguiente:

(i) que elija uno de los enteros y lo multiplique por 5,
(ii) que sume 7,
(iii) que multiplique por 2,
(iv) que sume el segundo entero y le diga el resultado.

De la explicación algebraica de este procedimiento, queda claro que lo único que se necesita es sustraer 14 del número dado como resultado por la persona para obtener un número cuyos dos dígitos son precisamente los enteros en cuestión.

(i) $5a,$
(ii) $5a + 7,$
(iii) $10a + 14,$
(iv) $10a + 14 + b.$

El juego de Nim (Ver Bibliografía Nº 50; págs. 16-19) puede analizarse completamente mediante los números binarios. Otro juego relacionado con números binarios (Bibliografía Nº 43; pág. 39) necesita k tarjetas para el caso en que se consideran números menores que 2^k. Todos los enteros positivos menores que 2^k tienen un desarrollo único como suma de potencias de dos en la forma

$$(\text{II} - 15) \qquad n = a_1 + a_2 \cdot 2 + a_3 \cdot 2^2 + \ldots + a_k \cdot 2^{k-1},$$

en donde $a_i = 0$ ó 1 $(i = 1, 2, \ldots, k)$. La primera tarjeta contiene todos los enteros positivos menores que 2^k para los cuales $a_1 = 1$, la segunda aquéllos para los cuales $a_2 = 1, \ldots$, las de orden k aquellos para los cuales $a^k = 1$. El primer número de la j-ésima carta es 2^{j-1}. Por consiguiente, para determinar un número, sólo se necesita saber en qué tarjeta aparece, es decir, las potencias de 2 que se utilizaron en su desarrollo binario. Cualquier persona que se familiarice con el juego puede, entonces, decir el número sin mirar las tarjetas, puesto que se ha dado su representación como número binario. El número deseado es la suma de los primeros números en cada una de las tarjetas donde aparece. Por ejemplo, si $k = 4$, tenemos las tarjetas

1	9
3	11
5	13
7	15

2	10
3	11
6	14
7	15

4	12
5	13
6	14
7	15

8	12
9	13
10	14
11	15

El número $5 = 1 + 0 \cdot 2 + 1 \cdot 2^2$ aparece sólo en la primera y tercera tarjeta. El número que aparece sólo en la segunda y tercera tarjeta es $0 \cdot 2^0 + 1 \cdot 2 + 1 \cdot 2^2 = 6$. El número que aparece sólo en la primera, tercera y cuarta tarjetas es $1 \cdot 2^0 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$. En general, la representación binaria del número es conocida tan pronto como se conocen las tarjetas en las cuales aparece el número, en (II - 15) $a_1 = 1$ si el número n está en la primera tarjeta, $a_1 = 0$ si n no está en la primera tarjeta. Asimismo, considerando $n < 16$ o un conjunto mayor de tarjetas que las dadas anteriormente, $a_i = 1$ en (II - 15) si n está en la tarjeta de orden i, de otro modo $a_i = 0$.

EJERCICIOS

1. Expresar 19 y 175 en base 2.
2. Expresar 95 y 348 en base 3.
3. Expresar 75 y 6789 en base 7.
4. En cada uno de los ejercicios anteriores, sumar los dos números usando la base nueva. Comprobar la adición sumando los dos números tal como se dieron en la base diez y expresando la suma en la base indicada.

5. Repetir el Ejercicio 4 efectuando la sustracción del segundo número menos el primero, en lugar de la adición.

6. Repetir el Ejercicio 4, efectuando la multiplicación.

7. Repetir el Ejercicio 4, efectuando la división del segundo número por el primero.

8. Expresar el número 12143_5 (el subíndice indica la base) en base 10 y en seguida en base 7.

9. Expresar 12143_5 en base 7 sin cambiarlo a base 10.

10. Proponer un método general para cambiar la base de cualquier entero. Ilustrar el método propuesto con tres enteros de por lo menos cinco dígitos cada uno y en donde todas las bases sean diferentes de diez.

11. Damos el siguiente ejemplo de la multiplicación campesina rusa de $43 \cdot 75$. Las partes enteras de los cuocientes sucesivos de 43 dividido por 2 están alineadas al lado de los múltiplos sucesivos de 75 multiplicado por 2. En seguida aquellos múltiplos de 75 que corresponden a cuocientes impares de 43 se suman para obtener el producto pedido.

43	75
21	150
(10)	(300)
5	600
(2)	(1200)
1	2400

$43 \cdot 75 = 75 + 150 + 600 + 2400 = 3225$. Representar en el sistema binario y proponer una demostración de la validez de este método.

12. Encontrar los siguientes productos por medio de la multiplicación campesina rusa $67 \cdot 85$; $73 \cdot 120$; $121 \cdot 373$.

13. La simplificación siguiente $\frac{16}{64}$ ofrece una respuesta correcta para la fracción $\frac{16}{64}$ en base diez. Encontrar, en base diez, todas las fracciones m/n, en donde $10 < m < 20$, y $10 < n < 100$, tales que después de efectuarse simplificaciones semejantes a la del Ejercicio 13, den una respuesta correcta.

14. Encontrar todas las fracciones m/n tales que m, n sean números de dos dígitos en base diez y que al simplificar como en el Ejercicio 13, resulte una respuesta correcta.

15. Demostrar que no hay fracciones como las que se piden en el Ejercicio 14, si los números se expresan en base p, en que p es un número primo.

II · 7 NOTACION DECIMAL. La representación de un número en base 10 se llama *notación decimal* del número. En el Capítulo II · 6 hemos encontrado que cualquier entero positivo m tiene una representación única en la notación decimal, es decir,

$$m = a_k 10^k + a_{k-1}10^{k-1} + \dots + a_1 10 + a_0,$$

en donde

$$\begin{aligned} m &= 10\, m_1 + a_0 \\ m_1 &= 10\, m_2 + a_1 \\ &\cdot \\ &\cdot \\ &\cdot \\ m_k &= 10 \cdot 0 + a_k \end{aligned}$$

y $0 \leqq a_i < 10$, $a_k \neq 0$.

Consideraremos ahora la representación en la notación decimal de los números racionales positivos s/n. Esta representación también está basada en el Algoritmo de la División. Por ejemplo, dado el número 51/8, podemos calcular

$$\begin{aligned} 51 &= 6 \cdot 8 + 3, \\ 30 &= 3 \cdot 8 + 6, \\ 60 &= 7 \cdot 8 + 4, \\ 40 &= 5 \cdot 8 + 0, \end{aligned}$$

y escribir $51/8 = 6.3750$. En general, dado cualquier número racional positivo s/n, podemos usar el Algoritmo de la División y escribir

$$s = mn + r,$$

en donde $0 \leqq m$ y $0 \leqq r < n$. El entero positivo m tiene un desarrollo decimal como en el caso anterior. El dígito de los décimos en el desarrollo decimal de r/n, y por lo tanto de s/n, es b_1, en que

$$10r = b_1 n + r_1,\ 0 \leqq r_1 < n.$$

El dígito de los centésimos es b_2, en que

$$10r_1 = b_2 n + r_2,\ 0 \leqq r_2 < n$$

y en general, para cualquier entero positivo j, el dígito j-ésimo hacia la derecha del punto decimal en el desarrollo de s/n es b_j, en donde

$$10r_{j-1} = b_j n + r_j,\ 0 \leqq r_j < n.$$

Queda por demostrar que se necesita únicamente un número finito de estas etapas para obtener la representación de s/n en la notación decimal.

En realidad, existe un conjunto infinito numerable de restos r_j $(j = 1, 2, \ldots)$ tal que $0 \leqq r_j < n$. Sin embargo, puesto que cada r_j es un elemento del conjunto $0, 1, 2, \ldots, n - 1$, hay solamente un número finito de valores distintos de los restos r_j. En efecto, deben existir enteros p, y $q = p + t$, en que t es positivo, tales que $r_{p-1} = r_{q-1}$, y por lo tanto

$$nb_p + r_p = nb_q + r_q,$$
$$n(b_p - b_q) = r_q - r_p$$

Puesto que los enteros positivos son bien ordenados, existen enteros positivos mínimos p y t que tienen las propiedades anteriores. Cualquier $p_1 > p$ y cualquier entero positivo múltiplo de t también tiene estas propiedades. Si $b_p = b_q$, entonces $r_q = r_p$. Si $b_p \neq b_q$, entonces n es divisor de $r_q - r_p$, en que $0 \leqq r_q < n$, $0 \leqq r_p < n$, y por lo tanto $r_q - r_p = 0 = b_p - b_q$, contrariamente a nuestra creencia de que $b_p \neq b_q$, tenemos que $b_p = b_q$ y $r_p = r_q$. De este modo hemos demostrado que existen enteros positivos diferentes p, q tales que $r_{p-1} = r_{q-1}$ y que esta igualdad implica $r_p = r_q$, es decir, $r_p = r_{p+t}$, en donde $q = p + t$. Finalmente, según el principio de inducción matemática, $r_j = r_{j+t}$ para todos los $j \geqq p - 1$ y el número positivo racional s/n puede escribirse en la forma:

$$a_k 10^k + \cdots + a_1 10 + a_0 + \frac{b_1}{10} + \frac{b_2}{10^2} + \cdots + \frac{b_p}{10^{p-1}} + \frac{c_1}{10^p} + \frac{c_2}{10^{p+1}} + \cdots$$

$$+ \frac{c_t}{10^{p+t-1}} + \frac{c_1}{10^{p+t}} + \frac{c_2}{10^{p+t+1}} + \cdots + \frac{c_t}{10^{p+2t-1}} + \frac{c_1}{10^{p+2t}} + \cdots$$

Hemos hecho una demostración completa de que todo número racional positivo puede representarse por un decimal periódico. En la práctica, como en la teoría, se procede como se hizo anteriormente para encontrar los r_j hasta que algún r_j sea cero, o sea, igual a algún r_k, en donde $k < j$. Por ejemplo, dado 153/7, se calcula

$$\begin{aligned} 153 &= 21 \cdot 7 + 6 \\ 60 &= 8 \cdot 7 + 4 \\ 40 &= 5 \cdot 7 + 5 \\ 50 &= 7 \cdot 7 + 1 \\ 10 &= 1 \cdot 7 + 3 \\ 30 &= 4 \cdot 7 + 2 \\ 20 &= 2 \cdot 7 + 6, \end{aligned}$$

de donde $153/7 = 21.857142857142\ldots$ Puesto que los decimales precedidos de signo se emplean para representar números precedidos de signo, todos los números racionales pueden representarse como fracciones periódicas. Recíprocamente, dado cualquier decimal d en el que se repiten una y otra vez t dígitos, podemos calcular el decimal finito $10^t d - d$ (Cap. I - 10) y expresar d como un número racional. De esta manera hemos demostrado que todo número racional puede expresarse como un decimal periódico, y viceversa. Los temas que siguen de este capítulo son importantes para la teoría de los números pero pueden suprimirse sin perturbar la organización de este texto.

EJERCICIOS

1. Emplear el método anterior de restos sucesivos y expresar cada uno de los siguientes números racionales en notación decimal:

$$\frac{1}{16},\quad \frac{1}{50},\quad \frac{3}{11},\quad \frac{2}{3},\quad \frac{1}{10},\quad \frac{1}{128}.$$

2. Repetir el Ejercicio 1 para $\frac{17}{3}$, $\frac{25}{8}$, $\frac{11}{6}$, $\frac{75}{16}$, $\frac{125}{36}$.

3. Demostrar que todo número racional puede representarse como un decimal periódico, valiéndose de que se obtienen a lo más q restos diferentes de los cuocientes $10^j/q$, en donde $j = 0, 1, 2, \ldots$.

4. Examinar el caso de la representación de números racionales en el sistema binario de números.

II-8* CONGRUENCIAS. Procederemos ahora a dividir el conjunto de los enteros en subconjuntos o subclases respecto a un entero m dado elegido arbitrariamente. Por ejemplo, de aquí a tres horas, de aquí a cincuenta y una horas, hace veintiuna horas, y, en general, $3 + 24k$ horas de ahora en adelante para cualquier entero k, todos representan la misma hora del día. Los números de horas, 3, 51, -21, $3 + 24k$ son equivalentes en cierto sentido respecto a un día de veinticuatro horas. Se dice que los números son congruentes módulo 24 y se escribe $3 \equiv 51$ (mód. 24). Asimismo, ángulos de 30°, 390°, $-330°$, 750°, y en general, $30° + (360k)°$ para cualquier entero k pueden representarse gráficamente utilizando los mismos lados inicial y terminal. Además, siempre que ángulos de $a°$ y de $b°$ puedan representarse utilizando los mismos lados inicial y terminal, tenemos que $a = b + 360\,k$ para algún entero k y se puede escribir $a \equiv b$ (mód. 360). En general se dice que dos enteros a y b son *congruentes módulo un entero* m si y sólo si existe un entero c que satisfaga la igualdad $a = b + cm$. Todas las veces que tal entero c exista, podemos escribir $a \equiv b$ (mód. m) y llamar a m el *módulo* de la congruencia. Esta definición es equivalente a la relación $a \equiv b$ (mód. m) si y sólo si $a - b$ es divisible por m. Por ejemplo $3 \equiv 8$ (mód. 5), $-3 \equiv 9$ (mód. 6), y dos enteros pares cualesquiera son congruentes módulo 2.

La congruencia módulo m es una relación de equivalencia (Cap. I-3), dado que es reflexiva, simétrica, y transitiva, es decir,

(i) $a \equiv a$ (mód. m),
(ii) $a \equiv b$ (mód. m) implica $b \equiv a$ (mód. m), y
(iii) $a \equiv b$ (mód. m) y $b \equiv c$ (mód. m) implican $a \equiv c$ (mód. m).

Es fácil demostrar estas tres propiedades basándose en las definiciones ya citadas: $a = a + 0m$; si $a = b + km$, entonces $b = a + (-k)m$; si $a = b + km$ y $b = c + hm$, entonces $a = c + (h + k)m$. La relación de equivalencia $=$ puede considerarse como un caso especial de $\equiv$, en que el $m = 0$. Sin embargo, en nuestro estudio nosotros vamos a admitir que $m \neq 0$.

Consideraremos en seguida algunas de las propiedades de esta nueva relación $\equiv$ (mód. m). Las congruencias módulo m pueden

combinarse empleando las operaciones del anillo: adición, sustracción, y multiplicación, es decir, si $a \equiv b$ (mód. m) y $c \equiv d$ (mód. m), entonces,

(II - 16) $$a + c \equiv b + d \pmod{m},$$
(II - 17) $$a - c \equiv b - d \pmod{m},$$
(II - 18) $$ac \equiv bd \pmod{m}.$$

Estas congruencias pueden demostrarse directamente basándose sobre la definición de congruencia. Si $a = b + sm$ y $c = d + tm$, entonces

$$a + c = b + d + (s + t)m,$$
$$a - c = b - d + (s - t)m,$$
y $$ac = bd + (bt + sd + stm)m,$$

en que $s + t$, $s - t$, y $bt + sd + stm$ son enteros, ya que el conjunto de los enteros es cerrado con respecto a las operaciones del anillo. La congruencia (II - 18) puede aplicarse para el caso especial de que $a = c$, $b = d$ y, por inducción matemática, resulta para cualquier entero positivo n

(II - 19) $$a^n \equiv b^n \pmod{m}.$$

Por ejemplo las congruencias $2 \equiv 7$ (mód. 5) y $3 \equiv 8$ (mód. 5) pueden sumarse y resulta $5 \equiv 15$ (mód. 5); pueden restarse y se obtiene $-1 \equiv -1$ (mód. 5); y multiplicarse para obtener $6 \equiv 56$ (mód. 5). También se puede elevar al cuadrado ambos miembros de la congruencia $2 \equiv 7$ (mód. 5) y se obtiene $4 \equiv 49$ (mód. 5).

Dado que para la formación de un polinomio sólo se necesitan operaciones anillo (Cap. III - 2), pueden aprovecharse las congruencias (II - 16), (II - 17), (II - 18), (II - 19) para obtener

TEOREMA II - 14. *Si $a \equiv b$ (mód. m) y $f(x)$ es un polinomio con coeficientes enteros, entonces $f(a) \equiv f(b)$* (mód. m).

Consideremos como un ejemplo de este teorema al polinomio $f(x) = x^3 - 3x^2 + 2x + 1$ y a la congruencia $2 \equiv -1$ (mód. 3), $f(2) = 8 - 12 + 4 + 1 = 1$ y $f(-1) = -1 - 3 - 2 + 1 = -5 \equiv 1$ (mód. 3).

También rige la ley cancelativa para las congruencias. Si $ak \equiv bk$ (mód. m), su diferencia es un múltiplo de m, es decir $(a - b)k = tm$. Sea $d = (k, m)$, entonces

$$(a - b)k/d = t(m/d) \text{ y } a \equiv b \quad (\text{mód. } m/d).$$

Por ejemplo, $2 \equiv 8$ (mód. 6) implica $1 \equiv 4$ (mód. 3); $12 \equiv 32$ (mód. 10) implica $6 \equiv 16$ (mód. 5) y $3 \equiv 8$ (mód. 5). Si $ak \equiv bk$ (mód. m) y $(k, m) = 1$, entonces $a \equiv b$ (mód. m). En general, se tiene.

TEOREMA II-15. *Si* $ak \equiv bk$ (mód. m) y $(k, m) = d$, *entonces* $a \equiv b$ (mód. m_1), *en que* $m = dm_1$.

Las congruencias pueden servir para dar pruebas de la divisibilidad de cualquier entero n por un entero m. Todo entero positivo puede expresarse unívocamente (Cap. II-6), en la forma (II-20)

$$\text{(II-20)} \qquad n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k,$$

en donde $0 \leq a_i \leq 9$ siendo $i = 1, 2, \dots, k$. La prueba tan familiar para la divisibilidad por 2 se encuentra considerando ambos miembros de (II-20) con respecto al módulo 2. Dado que $10 \equiv 0$ (mód. 2), podemos reemplazar 10, 10^2, ..., y 10^k por 0 en el caso de que se considere a n en (II-20) con respecto al módulo 2. Luego $n \equiv a_0$ (mód. 2), es decir, $n = a_0 + 2t$ para cualquier entero t, y n es divisible por 2 si y sólo si a_0 es divisible por 2. Asimismo, de $10 \equiv 1$ (mód. 3) y de la relación (II-19), se tiene $n \equiv a_0 + a_1 + \dots + a_k$ (mód. 3), es decir, n es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3. Puesto que $10^2 \equiv 0$ (mód. 4), se obtiene $n \equiv a_0 + 10a_1$ (mód. 4), en donde n es divisible por 4 si y sólo si el número compuesto por sus últimos dos dígitos es divisible por 4. También se puede usar (II-20) para obtener:

$$\begin{aligned}
& n \equiv a_0 \ (\text{mod } 5), \\
& n \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 \\
& \qquad + 3a_7 + 2a_8 - a_9 - \cdots \ (\text{mod } 7), \\
(2\text{–}21) \qquad & n \equiv a_0 + a_1 + \cdots + a_k \ (\text{mod } 9), \\
& n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \ (\text{mod } 11), \\
& n \equiv a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + a_6 \\
& \qquad - 3a_7 - 4a_8 - a_9 + \cdots \ (\text{mod } 13), \\
& n \equiv a_0 + 10a_1 \ (\text{mod } 25),
\end{aligned}$$

y muchas otras pruebas semejantes para la divisibilidad. Por ejemplo, $342538 \equiv 0$ (mód. 7), es decir, es divisible por 7, dado que $a_0 = 8$, $a_1 = 3$, $a_2 = 5$, $a_3 = 2$, $a_4 = 4$, $a_5 = 3$, y empleando la prueba que acabamos de señalar, $342538 \equiv 8 + 3 \cdot 3 + 2 \cdot 5 - 2 - 3 \cdot 4 - 2 \cdot 3 = 7 \equiv 0$ (mód. 7). De manera análoga, 3637425 es divisible por 11, y 7587125 es divisible por 13. La naturaleza periódica de los múltiplos de los dígitos a_i se examina en los Ejercicios 5 y 6, Cap. II-10.

Antes de la invención de la máquina de calcular, se revisaban muchos procedimientos aritméticos por el método de *calcular los nueves,* es decir, se consideraban los números con respecto al módulo 9 como en (II-21) y se empleaban las congruencias (II-16), (II-17), y (II-18). El producto $321 \cdot 152 = 48792$ se revisaría por medio de las congruencias $321 \equiv 6$ (mód. 9), $152 \equiv 8$ (mód. 9), $321 \cdot 152 \equiv 6 \cdot 8 \equiv 48 \equiv 3 \equiv 48792$ (mód. 9). Este método no es una revisión perfecta, ya que no se localizan algunos errores, como por ejemplo, el intercambio de dos dígitos. En el caso de un cuociente $a/b = q + r/b$, la relación $a = qb + r$ debe ser válida y se comprueba que $a \equiv qb + r$ (mód. 9). Por ejemplo, la ecuación $\frac{83}{17} = 4 + \frac{15}{17}$ se comprueba considerando que $83 = 4 \cdot 17 + 15$, lo que resulta $2 \equiv 4 \cdot (-1) + 6$ (módulo 9).

EJERCICIOS

1. Demostrar que $a^2 \equiv 1$ (módulo 8), en donde a es cualquier número impar.

2. Proponer cuatro ejemplos del Teorema II-14, usando polinomios de por lo menos tercer grado.

3. Encontrar $f(13)$ (mód. 9) si $f(x) = 7x^5 + 13x^4 - 72x^3 + 2153$.

4. Proponer tres ejemplos numéricos que ilustren el Teorema II-15.

5. Proponer pruebas de la divisibilidad por 6, 8 y 15.

6. Examinar si 1113 y 23,535 son divisibles por 7, 9, 11 y 15 usando los teoremas de congruencia.

7. Comprobar lo siguiente por el método de "calcular los nueves":

a) $1235 \cdot 341 = 421135$;
b) $852 + 1239 + 251 + 172 = 2514$.

8. Exponer un método para "calcular los onces". Repetir el Ejercicio 7, calculando los onces.

9. Encontrar una demostración de la divisibilidad por 4, de números expresados en base cinco. Proponer un ejemplo de tres dígitos y otro de cuatro dígitos.

10. Proponer una demostración de la divisibilidad por $n - 1$ para números expresados en base n.

11. Proponer una demostración de la divisibilidad por $n + 1$ para números expresados en base n.

12. Proponer demostraciones de la divisibilidad por 4, 8 y 16 y demostrar que se necesitan considerar cuando más b dígitos para probar la divisibilidad por 2^b de cualquier entero dado expresado en base 10.

13. Demostrar que $a \equiv b$ (mód. m), $0 < a < m$, $0 < b < m$, implica $a = b$.

14. Tres hermanos decidieron en el colegio repartir su caja común de bolitas entre los siete miembros de su pandilla. El primero de los tres hermanos que llegó a su casa repartió las bolitas en siete grupos y le sobró una bolita, tomó su pila y la bolita sobrante. El segundo hermano, llegó a su casa, repartió las bolitas restantes en siete pilas, le sobró una bolita que dio a su hermana y tomó su pila. Cuando el tercer hermano llegó a su casa, separó las bolitas restantes exactamente en siete pilas iguales. Encontrar el menor número posible de bolitas para el número original de bolitas. Dar todas las soluciones considerando el problema como clase de congruencia (Cap. II-9). (*Indicación:* Comenzar expresando el número pedido en base 7, por ejemplo, $N = abc_7$).

II-9* CLASES RESIDUALES. FUNCION ϕ DE EULER. Dados dos enteros cualesquiera c y m, el Algoritmo de la División establece que existen enteros q y r, $0 \leq r < m$, tales que $c = qm + r$. El número r se llama el *residuo* de c con respecto al módulo m y se escribe $c \equiv r$ (mód. m). Por ejemplo, $7 \equiv 2$ (mód. 5), $31 \equiv 1$ (mód. 5), $102 \equiv 2$ (mód. 5). La totalidad de los números c tales que $c \equiv r$ (mód. m) se llama *clase residual o clase de congruencia* con respecto al módulo m y se indica por $[r]$ (mód. m). Los números de la clase $[r]$ (mód. m), son

$$r,\ r \pm m,\ r \pm 2m,\ r \pm 3\ m,\ \ldots.$$

Por ejemplo, la clase residual [2] (mód. 5), comprende a los números

$$\ldots,\ -13,\ -8,\ -3,\ 2,\ 7,\ 12,\ 17,\ \ldots.$$

Todo entero positivo, negativo o cero pertenece, con respecto al módulo 5, a una de las clases residuales [0], [1], [2], [3], [4] (mód. 5). En general, todo entero pertenece, con respecto al mó-

dulo m, a una de las clases residuales $[0]$, $[1]$, $[2]$, ..., $[m-1]$ (mód. m) (ver Ejercicio 8). Para $m = 2$ todos los números pares pertenecen a la clase residual $[0]$ (mód. 2) y todos los números impares pertenecen a la clase residual $[1]$ (mód. 2). Un conjunto de números $r_1, r_2 \ldots r_m$, en que cada uno de ellos pertenece a cada una de las clases $[0]$, $[1]$, $[2]$, ..., $[m-1]$ (mód. m), se llama un *sistema residual completo,* con respecto al módulo m. Por ejemplo, los números 5 y 8 forman un sistema residual completo con respecto al módulo 2; los números 64, 17, 34, y -1 forman un sistema residual completo con respecto al módulo 4.

Una clase residual $[r]$ (mód. m) puede ser expresada en función de cualquiera de sus elementos, es decir, $[r]$ (mód. m) $= [r + km]$ (mód. m) para cualquier entero k. De este modo, para cualquier entero m el número total de clases residuales distintas con respecto al módulo m *es* $|m|$. Un conjunto de números $r_1, r_2, \ldots, r_m$ es un sistema residual completo con respecto al módulo m si y sólo si $r_i \not\equiv r_j$ (mód. m) siempre que $i \neq j$ *e* $i, j = 1\ 2, \ldots, m$.

Los sistemas residuales completos pueden usarse en la determinación de todas las raíces n-ésimas de la unidad a partir de una raíz n-ésima primitiva dada de la unidad. Por definición (Cap. I-17), s es una raíz n-ésima de la unidad si y sólo si n es el entero positivo menor k tal que $s^k = 1$. Luego si $s^m = 1$, podemos escribir $m = qn + r$, en donde $0 \leqq r < n$, y obtener $s^m = s^{qn+r} = s^{qn} \cdot s^r = s^r = 1$. Ahora, dado que $0 \leqq r < n$, $s^r = 1$ y n es el menor entero positivo k tal que $s^k = 1$, tenemos que $r = 0$ y $m = qn$, es decir, $s^m = 1$ si y sólo si $m \equiv 0$ (mód. n), en donde s es una n-ésima raíz primitiva de la unidad.

El Teorema de De Moivre (Cap. I-17) establece la existencia de por lo menos una raíz n-ésima primitiva de la unidad para cualquier entero positivo n. Dada una raíz s n-ésima primitiva de la unidad, resulta que, según (Cap. I-17), toda potencia entera de s, por ejemplo, s^t, era también una raíz n-ésima, dado que $(s^t)^n = (s^n)^t = 1^t = 1$. Además, si $s^t = s^u$, entonces $s^{t-u} = 1$ y $t - u \equiv 0$ (mód. n), es decir, $t \equiv u$ (mód. n). De aquí que dos potencias enteras de una raíz n-ésima primitiva de la unidad sean distintas si y sólo si los exponentes pertenecen a distintas clases residuales con respecto al módulo n. Después de esto, podemos generalizar el Teorema I-7, como sigue:

TEOREMA II-16. *Todas las n-ésimas raíces de la unidad están dadas por la sucesión*

$$s^{r_1}, s^{r_2}, \ldots, s^{r_n},$$

en donde s es una raíz n-ésima primitiva de la unidad y los r_i forman un sistema residual completo respecto al módulo n.

Por ejemplo, si $n = 4$, entonces 16, -11, 30, 67 forman un sistema residual completo y todas las raíces cuartas de la unidad pertenecen al conjunto $i^{16} = 1$, $i^{-11} = i$, $i^{30} = -1$, $i^{67} = -i$, en donde $i = \sqrt{-1}$.

Definiremos, en seguida, un segundo tipo de sistema residual, llamado sistema residual reducido.

El número de enteros positivos menores que o iguales a m y primos respecto de m, se denota por $\phi\ (m)$ para cualquier entero positivo m y se llama el indicador (totient) de m o *función ϕ de m de Euler*. Por eso, $\phi\ (m)$ es el número de enteros k del conjunto

(II-22) $\qquad 1, 2, 3, \ldots, m-1, m$

tal que $(k, m) = 1$; $\phi\ (2) = 1$, $\phi\ (3) = 2$, $\phi\ (4) = 2$, $\phi\ (5) = 4$, $\phi\ (6) = 2, \ldots$. De lo anterior y de la definición de números primos entre si (Cap. II-1), se obtiene $\phi\ (1) = 1$.

Si $(r, m) = 1$, entonces para cualquier entero k tenemos $(r + km, m) = 1$, es decir, todo elemento de $[r]$ (mód. m) es un número primo con respecto a m. Por consiguiente, una clase residual $[r]$ (mód. m) es *prima respecto de m* si y sólo si $(r, m) = 1$. Utilizaremos estas relaciones para definir un sistema residual reducido. Un conjunto de números $r_1, r_2, \ldots, r_{\phi(m)}$, en que cada uno de ellos pertenece a cada una de las clases residuales que son primas respecto de m, se llama un *sistema residual reducido* respecto del módulo m.

Este segundo tipo de sistema residual puede emplearse también en el estudio de las n-ésimas raíces de la unidad. Supongamos que s es una raíz n-ésima primitiva de la unidad, y consideremos que k sea tal que s^k sea una raíz n-ésima primitiva de la unidad. Entonces $(s^k)^n = 1$ para cualquier entero k, dado que s es una raíz n-ésima primitiva. Si $(k, n) = d > 1$, entonces $k = k_1d$, $n = n_1d$, en donde $n_1 < n$ y $(s^k)^{n_1} = (s^{k_1d})^{n_1} = (s^{n_1d})^{k_1} = 1^{k_1} = 1$, es decir,

s^k no es una raíz n-ésima primitiva si $(k, n) = d > 1$. Si $(k, n) = 1$ y $(s^k)^m = 1$, entonces $km \equiv 0$ (mód. n); es decir, $n \mid km$ y, según el Teorema II-9, $n \mid m$, de donde s^k es una raíz n-ésima primitiva de la unidad. Por consiguiente, s^k es una raíz n-ésima primitiva de la unidad si y sólo si $(k, n) = 1$. Esto nos permite encontrar todas las raíces n-ésimas primitivas dada una raíz n-ésima primitiva de la unidad.

TEOREMA II-17. *Si s es una raíz n-ésima primitiva de la unidad, entonces todas las raíces n-ésimas primitivas de la unidad pertenecen al conjunto*

$$s^{r_1}, s^{r_2}, \ldots, s^{r_{\phi(n)}},$$

en donde las r forman un sistema residual reducido con respecto al módulo n.

Usaremos también los sistemas residuales reducidos en las demostraciones del Teorema de Euler y del Teorema Simple de Fermat en la sección 10 de este Capítulo II.

EJERCICIOS

1. Escribir los sistemas residuales completos con respecto a los siguientes módulos enteros: 4, 5, 9, 11 y 16.

2. Escribir los sistemas residuales reducidos con respecto a los siguientes módulos enteros: 4, 5, 9, 11, 16, 31, 60, -70.

3. Demostrar que los números $-5, -2, 12, 26, 39, 53$ forman un sistema residual completo respecto al módulo 6.

4. Demostrar que m enteros consecutivos cualesquiera forman un sistema residual completo respecto al módulo m.

5. Demostrar que si $(d, m) = 1$, entonces $d, 2d, 3d, \ldots, md$ forman un sistema residual completo respecto al módulo m.

6. Demostrar que $a + r_1, a + r_2, a + r_3, \ldots, a + r_m$ es un sistema residual completo respecto al módulo m para cualquier entero a si $r_1, r_2, r_3, \ldots, r_m$ es un sistema residual completo respecto al módulo m.

7. Expresar un sistema residual completo respecto al módulo mn en que $(m, n) = 1$ en función de sistemas residuales completos dados de m y n.

8. Por medio del Algoritmo de la División demostrar que todo entero pertenece, respecto al módulo m, a una y solo una de las clases residuales $[0], [1], \ldots, [m - 1]$ (mód. m) en donde $m \neq 0$ es un entero arbitrario.

9. Definir $[a] + [b] = [a + b]$ respecto al módulo m; $[a] \cdot [b] = [ab]$ con respecto al módulo m, y demostrar que estas definiciones son independientes de los elementos particulares a, b elegidos de las clases residuales $[a]$, $[b]$ respecto al módulo m.

10. Demostrar que las clases residuales, módulo 5, forman un anillo.

11. Demostrar que las clases residuales, módulo 6, forman un anillo.

12. Demostrar que las clases residuales, módulo m para cualquier entero $m \neq 0$ forman un anillo.

13. Ilustrar el concepto de divisores cero (Cap. I-14) por medio de clases residuales respecto al módulo 6.

14. Demostrar que las clases residuales, módulo 5, forman un campo.

15. Demostrar que las clases residuales módulo p para cualquier número primo p forman un campo.

II-10* EVALUACION DE ϕ (m). Dado que todo entero positivo puede expresarse de una manera única como el producto de números primos (Teorema II-8) evaluaremos primero la función ϕ para los números primos. Si m es un número primo, entonces todo número, excepto m, en la relación (II-22) es primo respecto de m y $\phi(m) = m - 1$. Si $m = p^a$, en que p es un número primo, entonces en el conjunto 1, 2, 3, ..., p, $p + 1$, ..., $2p$, $2p + 1$, ..., $3p$, ..., p^a, sólo los números p, $2p$, $3p$, ..., $(p^{a-1})p$ son divisibles por p. Por consiguiente, $p^a - p^{a-1}$ de los números son primos respecto de p (Teorema II-5) y

$$\phi(p^a) = p^a\left(1 - \frac{1}{p}\right).$$

Demostraremos, en seguida, que si $m = uv$, en que $(u, v) = 1$, entonces $\phi(m) = \phi(u)\,\phi(v)$ y, en general, la función ϕ de un producto de factores primos entre sí, es igual al producto de las funciones ϕ de los factores. Esto puede demostrarse rápidamente teniendo en cuenta que hay exactamente $\phi(m)$ raíces m-ésimas primitivas de la unidad y que todas las raíces m-ésimas de la unidad forman un grupo cíclico (Cap. I-17). Se obtiene una demostración más larga, pero más elemental, escribiendo todos los enteros 1, 2, 3, ..., uv en una ordenación rectangular, como sigue:

1	2	3	$\ldots$	h	$\ldots$	u
$u+1$	$u+2$	$u+3$	$\ldots$	$u+h$	$\ldots$	$2u$
$2u+1$	$2u+2$	$2u+3$	$\ldots$	$2u+h$	$\ldots$	$3u$
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
$(v-1)u+1$	$(v-1)u+2$	$(v-1)u+3$	$\ldots$	$(v-1)u+h$	$\ldots$	$vu.$

Por ejemplo, si $u = 5$ y $v = 3$, se escribe:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15

Cada hilera forma un sistema residual completo respecto al módulo u. Cada columna forma parte de una sola clase residual (mód. u), es decir, todo elemento de la columna encabezada por el número h pertenece a $[h]$ (mód. u). Siendo así, los elementos de la columna encabezada por h son primos respecto de u, si y sólo si $(h, u) = 1$. El número de columnas cuyos elementos son primos respecto de u es, por lo tanto, $\phi(u)$. Demostraremos, en seguida, que en cada columna no hay dos elementos que pertenezcan a la misma clase residual respecto del módulo v. Consideremos $su + h$ y $tu + h$. Según el Algoritmo de la División,

$$su + h = q_s v + r_s, \quad 0 \leqq r_s < v,$$
$$tu + h = q_t v + r_t, \quad 0 \leqq r_t < v.$$

Supongamos que $r_s = r_t$, entonces $(s - t)u = (q_s - q_t)v$. Puesto que $(u, v) = 1$ y $u > 0$, o bien $q_s = q_t$ o bien v es divisor de $s - t$. Pero $s < v$, $t < v$ y según el Ejercicio 3, Cap. II - 1, se tiene $s = t$, es decir, no hay dos elementos distintos de ninguna columna determinada que sean congruentes respecto al módulo v. Ya que hay v elementos en cada columna, cada columna constituye un sistema residual completo respecto al módulo v y contiene exactamente $\phi(v)$ elementos que son primos respecto de v. Por consiguiente, en cada una de las $\phi(u)$ columnas de elementos primos respecto de u, hay $\phi(v)$ elementos que también son primos respecto de v, es decir, hay $\phi(u)\,\phi(v)$ elementos primos respecto de u y de v simultáneamente y, por consiguiente respecto de uv (Teorema II - 9). En

otras palabras, $\phi(uv) = \phi(u)\,\phi(v)$. En general, si $m_1, m_2, \ldots, m_k$ son k enteros positivos que son primos entre sí, entonces

$$\phi(m_1 m_2 \ldots m_k) = \phi(m_1)\,\phi(m_2)\ldots\phi(m_k).$$

De los dos últimos párrafos y del Teorema II - 8, resulta

TEOREMA II - 18. *Para cualquier entero positivo* $m = p_1^{a_1} \cdot p_2^{a_2} \ldots p_n^{a_n}$, *en que los* p *son números primos distintos,*

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right).$$

Por ejemplo: $\phi(15) = 15(1 - \frac{1}{3})(1 - \frac{1}{5}) = 8$

o también $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$.

Tenemos también el

TEOREMA II - 19. *Dados enteros positivos* m, n, d, *tales que* $m = nd$, *el número de enteros* $k \leqq m$ *tal que* $(k, m) = d$, *es* $\phi(n)$.

Esto se demuestra fácilmente, ya que todo número $\leqq m = nd$ que tenga un divisor d es uno del conjunto $d, 2d, 3d, td, \ldots, (n-1)d, nd$ y $(td, m) = d$ o también $(td, nd) = d$ si y sólo si $(t, n) = 1$. Por consiguiente, el número de valores de t, tales que $(td, m) = d$ es exactamente $\phi(n)$.

El valor de $\phi(m)$ para cualquier entero positivo m puede encontrarse por medio del Teorema II - 18. Para $m \leqq 10{,}000$ estos valores se encuentran en un conjunto de tablas cuyo autor es J. W. L. Glaisher.

El siguiente teorema proporciona una aplicación muy importante de la función ϕ (ver Bibliografía Nº 43; págs. 272-310).

TEOREMA II - 20. TEOREMA DE EULER. *Si* m *es un entero positivo y* a *es cualquier entero tal que* $(a, m) = 1$, *entonces* $a^{\phi(m)} \equiv 1$ (*mód.* m).

Si m es un número primo p, este teorema se convierte en el Teorema formulado con anterioridad, por Fermat.

TEOREMA II - 21. TEOREMA SIMPLE DE FERMAT. *Si* p *es un número primo y* $p \nmid a$, *entonces* $a^{p-1} \equiv 1$ (mód. p).

El Teorema II - 21 se expresa con frecuencia en la forma $a^p \equiv a$ (mód. p) que es válida para todos los enteros positivos a.

Una demostración del Teorema II - 20 y por lo tanto también del Teorema II - 21, supone un sistema residual reducido con respecto al módulo m, por ejemplo $r_1, r_2, \ldots, r_{\phi(m)}$. Dado que por hipótesis $(a, m) = 1$, el conjunto de elementos $ar_1, ar_2 \ldots, ar_{\phi(m)}$ también constituye un sistema residual reducido respecto al módulo m. Por lo tanto, los elementos de los dos sistemas deben ser congruentes módulo m en pares (siguiendo alguna ordenación) y por medio de la aplicación repetida de la relación (II - 18), tenemos

$$a^{\phi(m)} r_1 r_2 \ldots r_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod{m}.$$

Por definición de un sistema residual reducido $(r_i, m) = 1$, en que $i = 1, 2, \ldots \phi(m)$. Siendo así, según el Teorema II - 15, podemos dividir ambos miembros de la ecuación anterior por $r_1 r_2 \ldots r_{\phi(m)}$ y obtenemos $a^{\phi(m)} \equiv 1 \pmod{m}$. Con esto se completa nuestra demostración del Teorema II - 20 y también del Teorema II - 21. En las dos últimas partes de este capítulo estudiaremos congruencias lineales y problemas diofánticos.

EJERCICIOS

1. Encontrar $\phi(12)$, $\phi(32)$, $\phi(17)$, $\phi(31)$, $\phi(60)$.
2. Demostrar que $(n-1)! \equiv 0 \pmod{n}$, en donde n es cualquier número compuesto diferente de 4.
3. Demostrar que $(a+b)^p \equiv a^p + b^p \pmod{p}$, en donde a y b son enteros cualesquiera y p es cualquier número primo.
4. Verificar el Teorema de Euler para $a = 7$ y $m = 12$.
5. Si $(m, 10) = 1$, demostrar que en la prueba para la divisibilidad por m de cualquier número suficientemente grande expresado en base 10, los múltiplos de los dígitos deben aparecer en conjuntos muy parecidos a los dígitos de un decimal periódico. Por ejemplo, $10^2 \equiv 1 \pmod{11}$ y $n \equiv a_0 - a_1 + a_2 - a_3 + \ldots \pmod{11}$, donde los múltiplos son el conjunto $+1$, -1 repetido hasta que se hayan considerado todos los dígitos del número dado.
6. Si $(m, 10) \neq 1$, hacer $m = 2^a 5^b n$ y valiéndose del Ejercicio 3, Cap. II-7, demostrar que para cualquier número m suficientemente grande, los múltiplos de los dígitos aparecen en conjuntos que se repiten después de haber considerado cierto número finito de dígitos.

II - 11* CONGRUENCIAS LINEALES.

La aritmética se preocupa principalmente de números. En álgebra se introducen nuevos símbolos llamados *variables* (Cap. III - 1).

Ahora nos apartaremos momentáneamente de la aritmética y volveremos al álgebra. Según la teoría de las ecuaciones, podemos considerar el problema de encontrar enteros x que satisfagan una congruencia de polinomios $f(x) \equiv 0 \pmod{m}$. Si a es un entero tal que $f(a) \equiv 0 \pmod{m}$ y $a \equiv b \pmod{m}$, entonces, según el Teorema II - 14, tenemos $f(b) \equiv 0 \pmod{m}$ y existe un conjunto de enteros infinito numerable

$$a, a \pm m, a \pm 2m, a \pm 3m, \ldots$$

que satisface la congruencia $f(x) \equiv 0 \pmod{m}$. Se habla de la clase residual completa $[a] \pmod{m}$ como la única *solución* de la congruencia de polinomios. De esta manera el número de soluciones de $f(x) \equiv 0 \pmod{m}$ es el número de clases residuales $[r_1]$, $[r_2]$, $\ldots$, $[r_k] \pmod{m}$ tales que $f(r_i) \equiv 0 \pmod{m}$. Dado que existen exactamente m clases residuales distintas, cualquier congruencia de polinomios dada tiene máximo m soluciones respecto al módulo m.

En el anillo de los enteros, puede dividirse ambos miembros de la ecuación $ax = b$ (Cap. II - 1) por a si y sólo si existe un entero c tal que $ac = b$. De manera análoga, la divisibilidad de ambos miembros de una congruencia respecto al módulo m por un entero se relaciona con la solución de una congruencia lineal $ax \equiv b \pmod{m}$. Por consiguiente se buscan valores enteros de la variable x que satisfagan

(II - 23) $\qquad ax \equiv b \pmod{m}$.

Estudiaremos primero un caso especial de (II - 23). La congruencia

(II - 24) $\qquad ax \equiv 1 \pmod{m}$

es válida si y sólo si $ax = 1 + km$ o si $ax - km = 1$ para algún entero k. Entonces, según el Teorema II - 12, $ax \equiv 1 \pmod{m}$ si y sólo si $(a, m) = 1$. Por consiguiente, (II - 24) tiene una solución única si y sólo si $(a, m) = 1$. Cuando (II - 24) tiene una solución única $[b] \pmod{m}$ cualquier elemento de $[b]$ se llama *recíproco* a^{-1} de a con respecto al módulo m. En consecuencia, un entero a tiene un recíproco respecto al módulo m si y sólo si $(a, m) = 1$. Por ejemplo: 3 es recíproco de 2 con respecto al módulo 5; 4 es recíproco de 2 con respecto al módulo 7, pero 2 no tiene recíproco

con respecto al módulo 6. Siempre se puede encontrar por medio del Teorema II - 12, un recíproco de n respecto al módulo de m, en caso de que exista, dado que si $(n, m) = 1$ existen enteros A y B tales que $Am + Bn = 1$, y B es el recíproco de n con respecto al módulo m.

Consideraremos ahora la congruencia (II - 23). Si $(a, m) = 1$, entonces a tiene un recíproco a^{-1}, y podemos escribir $a^{-1}ax \equiv a^{-1}b$ (mód. m), $x \equiv a^{-1}b$ (mód. m). De esta manera (II - 23) tiene una solución si $(a, m) = 1$. En general, si $(a, m) \mid b$, se hace $(a, m) = d$; $a = a_1d$; $m = m_1d$; y $b = b_1d$. Luego $(a_1m_1) = 1$ y $a_1x \equiv b_1$ (mód. m_1) tiene una solución $x \equiv a_1^{-1}b_1$ (mód. m_1), es decir, $a_1x = b_1 + km_1$ para algún entero k. De esta ecuación obtenemos $a_1dx = b_1d + km_1d$, o $ax = b + km$, de donde (II - 23) tiene una solución si $(a, m) \mid b$. A la inversa, si $ax \equiv b$ (mód. m) tiene una solución $[r]$ (mód. m), entonces $ar = b + km$ para algún entero k, de donde $ar - km = b$ y $(a, m) \mid b$. Es así como $ax \equiv b$ (mód. m) tiene siempre solución si $(a, m) = 1$ y en general, tenemos el

TEOREMA II - 22. *La congruencia* $ax \equiv b$ (mód. m) *tiene solución si y sólo si* $d = (a, m)$ *es divisor de* b.

Por ejemplo, $2x \equiv 1$ (mód. 6) y $3x \equiv 5$ (mód. 6) no tiene soluciones; $2x \equiv 1$ (mód. 5) y $3x \equiv 9$ (mód. 6) tienen solución.

Si $ax \equiv b$ (mód. m), y $ay \equiv b$ (mód. m), entonces $ax \equiv ay$ (mód. m), y también $ax = ay + km$. Como anteriormente, sea $d = (a, m)$; $a = da_1$, $m = dm_1$. Entonces $a_1(x - y) = km_1$ y $x \equiv y$ (mód. m_1). De aquí que dos soluciones cualesquiera de (II - 23) sean congruentes con respecto al módulo m_1. Si $[x]$ (mód. m) es una solución de (II-23), entonces, valiéndonos de $b = db_1$, tenemos $a_1dx = b_1d + kdm_1$, de donde $a_1x = b_1 + km_1$, es decir, cualquiera solución de (II - 23) es una solución de $a_1x \equiv b_1$ (mód. m_1). Según el Teorema II - 22, $a_1x \equiv b_1$ (mód. m_1) tiene una solución $[x_0]$ (mód. m_1) que, según la demostración anterior, es única. Por consiguiente, todas las soluciones de (II - 23) pertenecen a $[x_0]$ (mód. m_1), es decir, al conjunto.

$$x_0, x_0 \pm m_1, x_0 \pm 2m_1, \ldots, x_0 \pm dm_1, \ldots$$

Dado que $x_0 + dm_1 \equiv x_0$ (mód. m), hay exactamente d soluciones (mód. m), a saber $[x_0]$, $[x_0 + m_1]$, $\ldots$, $[x_0 + (d - 1)m_1]$ (mód. m). Por eso tenemos el

TEOREMA II - 23. *Si* $ax \equiv b$ (mód. m) *tiene una solución, entonces hay una solución única* (mód. m/d) *en donde* $(a, m) = d$, y d *soluciones* (mód. m).

Por ejemplo, $6x \equiv 9$ (mód. 15) tiene una sola solución [4] (mód. 5) y tres soluciones [4], [9], [14] (mód. 15) en donde $d = (6, 15) = 3$.

Resultados análogos al anterior pueden obtenerse para congruencias simultáneas respecto de varios módulos (ver Bibliografía Nº 43; págs. 240-249). En particular el Teorema Chino de los Restos se presta para muchos problemas interesantes. [Si los enteros $m_1, m_2, \ldots, m_t$ son primos por pares, existen enteros x para los cuales simultáneamente $x \equiv a_1$ (mód. m_1); $x \equiv a_2$ (mód. m_2), ..., $x \equiv a_t$ (mód. m_t)]. Sin embargo, en un tratado breve como el presente, deben suprimirse muchos detalles. Por este motivo, consideramos que hemos cumplido con nuestra finalidad de presentar conceptos básicos de congruencias lineales y dejamos que el lector prosiga el estudio de algunas interesantes aplicaciones, como la mencionada anteriormente, en textos dedicados enteramente a la teoría de los números.

EJERCICIOS

1. Demostrar que la factorización no es necesariamente única (mód. m) cuando m no es un número primo, mostrando dos factorizaciones distintas de $x^2 - 1$ con respecto al módulo 15.
2. Resolver las congruencias:
   a) $x^2 - 6x + 5 \equiv 0$ (mód. 4);
   b) $x^5 + 2x^2 + 4x + 3 \equiv 0$ (mód. 5).
3. ¿Cuántas soluciones tiene la congruencia $x^{17} \equiv x$ (mód. 17)?
4. Resolver la congruencia $x^7 + 2x^6 + 8x^4 + x + 3 \equiv 0$ (mód. 5).
5. Encontrar el recíproco de 7 (mód. 13), de 5 (mód. 33) y de 12 (mód. 49).
6. Resolver cuando sea posible:
   a) $4x \equiv 1$ (mód. 5);
   b) $4x \equiv 1$ (mód. 6);
   c) $6x \equiv 39$ (mód. 15);
   d) $6x \equiv 39$ (mód. 34);
   e) $1250x \equiv 1725$ (mód. 2000).
7. Encontrar todas las soluciones de las siguientes congruencias:
   a) $4x \equiv 6$ (mód. 10);
   b) $10x \equiv 8$ (mód. 16).

8. Demostrar el Teorema de Wilson: $(p-1)! \equiv -1$ (mód. p), para cualquier número primo p.

9. Demostrar que dos congruencias $x \equiv a$ (mod. m) y $x \equiv b$ (mód. n) tienen una solución común si y sólo si $a \equiv b$ (mód. s), en donde $s = (m, n)$. (Ver Bibliografía Nº 43; págs. 241-242). Proponer un método para encontrar la solución en caso de que exista.

II - 12* PROBLEMAS DIOFANTICOS. Terminaremos nuestro breve estudio de la teoría de los números, citando dos famosos problemas. El primero se refiere a las soluciones enteras de la *ecuación de Pitágoras* $a^2 + b^2 = c^2$; el segundo se conoce con el nombre de Ultimo Teorema de Fermat. Ambos problemas se refieren a soluciones enteras y pueden llamarse problemas *diofánticos,* es decir, problemas algebraicos en los que se piden soluciones racionales. Estos problemas se incluyen en la mayoría de los textos sobre teoría de los números, por ejemplo en (Bibliografía Nº 43; págs. 165-208) y (Bibliografía Nº 50; págs. 37-67 y 388-428).

La ecuación pitagórica es una expresión algebraica del *teorema de Pitágoras* que dice que en un triángulo rectángulo la suma de los cuadrados cuyos lados son iguales a los catetos es igual al cuadrado cuyo lado tiene la misma longitud que la hipotenusa. El problema de encontrar todas las soluciones enteras de la ecuación pitagórica, se convierte precisamente en el problema de encontrar todos los triángulos rectángulos cuyos lados tengan longitudes enteras. La solución particular $a = 3$, $b = 4$, $c = 5$, junto con $a = 5$, $b = 12$, $c = 13$ y con $a = 8$, $b = 15$, $c = 17$, era conocida por los escritores chinos, hindúes y egipcios de la antigüedad. Los griegos atribuyen a Pitágoras una solución algo más general

$$a = 2n + 1,\ b = 2n^2 + 2n,\ c = 2n^2 + 2n + 1, \qquad \text{(II - 25)}$$

donde n es cualquier entero.

Podemos verificar fácilmente, por sustitución, que (II - 25) es una solución para cualquier entero n. Sin embargo, la relación $b + 1 = c$ que debe ser válida para todas las soluciones que se obtienen de (II - 25), no necesita ser válida para todas las soluciones de la ecuación pitagórica. Por ejemplo, $a = 8$, $b = 15$, $c = 17$ es una solución que no se puede obtener de (II - 25). Muchas otras soluciones como ésta resultan del hecho de que si a, b, c es una solu-

ción de la ecuación pitagórica, entonces *da, db, dc* es también una solución para cualquier entero *d*. De aquí que (II - 25) no proporcione todas las soluciones de la ecuación pitagórica o aún todas las soluciones tales que *a, b* y *c* sean primos entre sí, es decir, *sean soluciones primitivas.* Todas las soluciones primitivas de la ecuación pitagórica se dan en las fórmulas. (Ver Bibliogr. Nº 50; pág. 40).

(II - 26) $\quad a = r^2 - s^2,\ b = 2rs,\ c = r^2 + s^2,$

en donde $(r, s) = 1,\ 0 < s < r,\ r \not\equiv s$ (mód. 2).

El otro problema que mencionaremos ha sido un constante desafío para los matemáticos por más de trescientos años.

TEOREMA II - 24. ULTIMO TEOREMA DE FERMAT. *Si n es un entero mayor que 2, no existen enteros x, y, z, tales que* $x^n + y^n = z^n$, *siendo* $xyz \neq 0$.

Fermat concibió este teorema como una extensión de la ecuación pitagórica (ver Bibliografía Nº 43; págs. 203-207) y señaló que tenía "una demostración verdaderamente maravillosa" de él, pero nunca formuló la demostración. Aun cuando se han ofrecido importantes premios por una demostración y aunque el teorema ha sido probado para todos los $n \leqq 617$, aún no se ha hallado una demostración general.

H. S. Vandiver hizo en 1946, una síntesis de todo lo relacionado con este teorema hasta esa fecha. (Ver Bibliografía Nº 51).

En todo este capítulo hemos considerado las propiedades del anillo de los enteros. La divisibilidad y el Algoritmo de la División se utilizaron en el estudio de los números primos, de la factorización única, y en el Algoritmo de Euclides. Se ha examinado también la representación de números en diversas bases. En la notación decimal se vio que todo número racional puede representarse en forma de decimal periódico y a la inversa. Se utilizó el concepto de una congruencia con respecto a un módulo entero *m* para verificar varios métodos corrientes de comprobar la divisibilidad y los cálculos aritméticos. También se empleó este concepto para subdividir el conjunto de enteros en clases residuales o de congruencia. El concepto de clase residual nos llevó a aquél de un sistema residual completo respecto al módulo *m* que comprende exactamente un

elemento de cada clase. Se descubrió en seguida que en cualquier sistema residual completo con respecto al módulo m, los elementos primos respecto de m constituían un sistema residual reducido respecto al módulo m. Dada una raíz m-ésima primitiva de la unidad, se obtuvieron todas las raíces m-ésimas por medio de cualquier sistema residual completo respecto al módulo m, y todas las m-ésimas raíces primitivas por medio de cualquier sistema residual reducido respecto al módulo m. Las propiedades de un sistema residual reducido sirvieron para demostrar dos teoremas clásicos en la teoría de los números, el Teorema de Euler y el Teorema Simple de Fermat. Finalmente, nos hemos referido de modo breve a las congruencias lineales y a los problemas diofánticos. Nuestro propósito ha sido principalmente presentar unos cuantos conceptos fundamentales y de este modo ofrecer en particular una mejor interpretación de las propiedades y comportamiento de los enteros a los lectores que no tengan la oportunidad de emprender un curso completo en este aspecto de las matemáticas. En el capítulo siguiente volveremos a considerar muchas de las propiedades del anillo de los enteros como propiedades de un anillo de polinomios.

EJERCICIOS

1. Demostrar que todas las soluciones primitivas de la ecuación pitagórica están dadas por las relaciones (11-26). (Ver Bibliografía Nº 50; págs. 38-40).

2. Hacer una lista de los veinte triángulos rectángulos que es posible obtener con los tres lados de longitudes enteras y el mayor de una longitud que no sobrepase las cincuenta unidades.

3. En una clase de 12 niños tienen b manzanas por cada niño para el almuerzo. En otra clase de 8 niños tienen c naranjas por niño. Encontrar dos pares posibles de valores de b y c, tales que los niños de las dos clases puedan hacer un intercambio de las frutas y distribuirlas equitativamente. ¿Cuáles son los valores positivos menores posibles de b y c? Proponer una solución completa del problema utilizando clases de congruencia.

4. Discutir la obra y métodos de Diofanto de Alejandría.